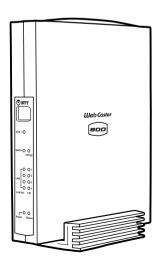
Web Caster 800

機能詳細取扱説明書

このたびは、Web Caster 800をお買い求めいただきまして、まことにありがとうございます。

●ご使用の前に、この「機能詳細取扱説明書」をよくお読みのうえ、内容を理解してからお使いください。

●お読みになったあとも、本商品のそばなどいつも手もとに置いてお使いください。

技術基準適合認証品

はじめに

この機能詳細取扱説明書では、取扱説明書で触れていない本商品の機能について解説しています。

※Microsoft®、Windows®は、米国Microsoft® Corporationの米国およびその他の国における登録商標または商標です。
※Windows®の正式名称は、Microsoft® Windows® Operating Systemです。
※Windows® XPは、Microsoft® Windows® XP Home Edition operating system およびMicrosoft® Windows® XP Professional operating system の略です。
※Windows® 2000 は、Microsoft® Windows® 2000 Professional operating system の略です。
※Windows Me® は、Microsoft® Windows® Millennium Edition operating system の略です。
※Windows 98® は、Microsoft® Windows® 98 operating system の略です。
※本書では、Windows® 98とWindows® 98 SEを含めて、Windows® 98と表記しています。
※Netscape®、Netscape Navigator® およびNetscape® Communicator は、米国Netscape® Communications Corporation の米国およびその他の国における登録商標または商標です。
※Macintosh®、Mac®、Mac OS® は、米国Apple Computer,Inc.の米国およびその他の国における登録商標です。
※本書では、Mac OS® X 10.0、10.1、10.2、10.3を、Mac OS® Xと表記しています。
また、Mac OS® 9.0、9.1、9.2を、Mac OS® 9.xと、Mac OS® 8.5、8.6をMac OS® 8.xと表記しています。
※Adobe® Acrobat® Reader™ は、Adobe® Systems Incorporated （アドビシステムズ社）の米国およびその他の国における登録商標または商標です。
※Java® は、米国Sun Microsystems,Inc.の米国およびその他の国における登録商標です。
※その他、本文中での記載の会社名および商品名およびロゴは各社の商標または登録商標です。
※付属品のCD-ROM は日本語版OS 以外の動作保証はしていません。
※付属品のCD-ROM はソフトウェアのバックアップとして保有する場合に限り、複製することができます。また、ソフトウェアについてのいかなる改変も禁止とし、それに起因する障害について当社は一切の責任を負いません。

目次

⑥ Web Caster 800 機能・詳細設定

⑦ 具体的な設定例

⑧ 資料

第6章 Web Caster 800 機能・設定詳細

この章では、Web Caster 800の機能について詳細に解説します。

Web Caster 800の主な機能

機能およびその概要の一覧

■ WAN側の機能

PPPoE機能	Bフレッツ、フレッツ・ADSLに対応。本体にPPPoE機能を搭載していますので、インターネット接続時はフレッツ接続ツール等を利用せずに自動接続できます。また、無通信の時間を監視して自動切断する機能もあり、より快適なインターネットアクセスを提供します。
複数PPPoE接続機能	ISPとフレッツ・スクエア等、同時に複数のPPPoE接続先に接続可能です。
Unnumbered機能	ISP事業者提供の複数固定IPアドレスサービスに対応し、サーバ（WWW・メール・FTP等）をインターネット上に公開できます。
ステートフルパケットインスペクション機能	ファイアウォールを通過するパケットのデータを読み取り、そのパケットとLAN側から送信したパケットとの間に矛盾がないかを判断し、動的にポートを開放・閉鎖します。
パケットフィルタリング機能	IPアドレス・ポート番号指定により不適切なパケットや不正なパケットを遮断し、パソコンを不正なアクセスから守ります。
DoS攻撃検出機能	WAN側からの不正な攻撃を検出し遮断します。
ローカルサーバ機能	ポート番号別に転送先のパソコンを指定し、サーバ（WWW、メール、FTP等）をインターネット上に公開できます。
DMZ機能	LAN上の1台のPCをインターネット側からアクセスできるようにします。1対1の通信を必要とするようなオンラインゲームやチャットソフト等に最適です。また、インターネットでの通信形態（ポート番号）が不明な場合にも有効です。 ※ DMZ機能利用時には、ファイアウォール機能が無効になり、セキュリティが弱くなります。必要な時だけ有効にしてください。

URL フィルタ機能	LAN 側に接続されてるパソコンからインターネットへのアクセスを制限します。
リモートアクセス機能	遠隔地のパソコンから Web サーバ、FTP サーバ、USB カメラにアクセスしたり、本商品の設定ができます。
VPN 機能	PPTP/IPSec による仮想プライベートネットワークが構築できます。
PPPoE ブリッジ機能	本機能を利用することで、LAN 側に接続したパソコンが直接 PPPoE 接続して通信することができます。本機能を利用してパソコンに直接グローバルアドレスを割り当てることによって、NAPT によるアドレス変換を行うことで使用できないアプリケーションが使用できるようになります。 ※ただし、WAN/LAN 間でのスループットは低下する場合があります。
IPv6 ブリッジ機能	IPv6 パケットのみ無条件で WAN 側と LAN 側をブリッジする機能です。IPv6 ネットワークを WAN 側に接続した場合は、ルータが介在することを気にせずに LAN 側に接続されたネットワークで IPv6 による通信を行うことが可能です。 ※ただし、IPv6 パケットの WAN/LAN 間でのスループットは低下する場合があります。
VPN パススルー機能	本商品の LAN 側に NAPT 環境で接続された VPN 機器から、WAN 側に設置された VPN 機器に対して IPSec および PPTP による接続ができる機能です。 ※ VPN サーバとして、本商品を用い IPSec/PPTP のクライアントとして Windows® XP を用いて検証を行っております。それ以外の構成については、保証の範囲外となりますのでご注意ください。

■ LAN 側の機能

NAPT 機能	ISP より提供されるグローバル IP アドレスを LAN 側のプライベートアドレスに変換します。これにより、LAN 側の複数のパソコンから同時にインターネットが利用できます。
DHCP サーバ機能	LAN 側のパソコンへ自動的に IP アドレスを割り当てます。 ※手動による IP アドレスの設定も可能です。
DNS サーバ機能	LAN 側のホスト名と IP アドレスを管理し、ホスト名から IP アドレスを参照できるようにします。

プロキシ DNS 機能	LAN 側のパソコンからの DNS 問い合わせのパケットを WAN 側の DNS サーバに転送します。
ダイナミックルーティング	動的にルーティング情報を設定し、大規模なネットワークにも対応します。 ※本商品は RIPv1/v2 に対応しています。
UPnP 機能	Windows Messenger 等の UPnP 対応アプリケーションを利用することができます。

■その他機能

サーバ機能	本商品の USB ポートに USB ストレージデバイス（USB ハードディスクや USB フラッシュメモリ等）を接続することにより、LAN 内ではファイルサーバとして、WAN 側に対してはWeb サーバ/FTP サーバとして動作します。 また、PHP に対応した Web サーバも動作します。（この機能は別途追加機能パッケージを追加する必要があります）
PHP スクリプト自動起動機能	本商品の USB ストレージ上に、“ startup ”というファイル名の PHP スクリプトを配置することで、本体起動時に自動的にそのスクリプトが実行されます。
USB カメラ機能	オプションの USB カメラ EE260 を本商品の USB ポートに接続することで、カメラサーバとして利用することができ、LAN 内やインターネット経由で撮影された静止画や動画が観覧できます。（この機能は別途追加機能パッケージを追加する必要があります）
ダイナミック DNS 機能	外部にサーバを公開する場合、本商品に動的な IP アドレスが割り当てられると、ホスト名と IP アドレスの連結ができなくなります。ダイナミック DNS 機能により変動する IP アドレスと固定のホスト名を結びつけることができ、公開サーバへのアクセスが容易になります。
Web ブラウザによるかんたん設定	専用ソフトウェアや専門的な知識が必要なコマンド入力が不要で、Web ブラウザによるかんたん設定で初心者の方でも短時間でセットアップができます。
E-mail 通知機能	アクセス制限ログ等を E-mail にて通知することができます。

設定ページの開き方

設定ページのアクセス方法

本商品は、Microsoft® Internet Explorer や Netscape Navigator® などの Web ブラウザで「設定ページ」を開いて、各種設定を行います。

起動の方法

1 パソコンを起動します。

2 本商品とパソコンが接続されていることを確認します。

3 Web ブラウザを起動します。

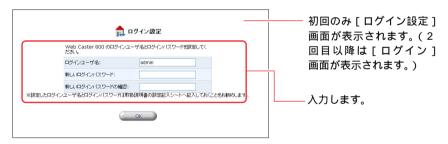
4 本商品の設定ページを開きます。アドレス欄に「http://192.168.1.1/」あるいは「http://wbc800.home/」と入力します。

※パソコンの DNS サーバアドレスに、プロバイダから指定されたアドレスを設定している場合は、アドレス欄に「http://192.168.1.1/」と入力してください。

5 キーボードの［Enter］キーを押します。

ログインユーザ名・ログインパスワードの設定方法

1　**本商品の設定ページを初めて開いたときは、下記の画面が表示されます。［OK］ボタンをクリックします。**

2　**本商品のログインユーザ名とログインパスワードを設定します。［ログインユーザ名］に任意の名前を入力し、［新しいログインパスワード］に任意のパスワードを入力します。確認のために［新しいログインパスワードの確認］に再度パスワードを入力します。**

［ログインユーザ名］

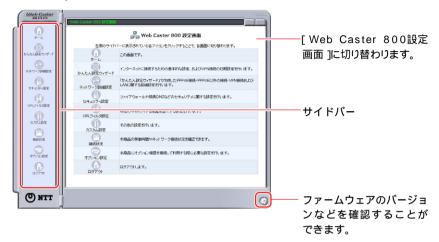
任意のユーザ名を入力します。半角英字または数字を使用し、1～64文字の範囲で入力してください。

［新しいログインパスワード］

任意のパスワードを入力します。半角英字または数字を使用し、1～64文字の範囲で入力してください。なお、入力したパスワードはすべて「＊」または「・」で表示されます。

［新しいログインパスワードの確認］

［新しいパスワード］と同じパスワードを再度入力します。
なお、入力したパスワードはすべて「＊」または「・」で表示されます。

3 **[OK]ボタンをクリックすると、Web Caster 800の設定画面が表示されます。**

設定メニューについて

ここでは、設定ページの各項目の概要を説明します。

■［ホーム］アイコン
クリックすると、［Web Caster 800 設定画面］に切り替わります。

■［かんたん設定ウィザード］アイコン
クリックすると、かんたん設定ウィザードが起動します。

■［ネットワーク詳細設定］アイコン
WAN ポートや LAN ポートの接続に関する詳しい設定を行う時に使用します。
クリックすると、［ネットワーク詳細設定］画面に切り替わります。

■［セキュリティ設定］アイコン
ファイアウォールの設定や、インターネットと LAN でのアクセス制限に関する設定を行うときに使用します。
クリックすると、［セキュリティ設定］画面に切り替わります。

■［URL フィルタ設定］アイコン
特定の Web サイトを閲覧禁止にするときに使用します。
クリックすると、［URL フィルタ設定］画面に切り替わります。

■［カスタム設定］アイコン
その他の設定を行うときに使用します。カスタム設定で行なう項目は次の通りです。

カスタム設定メニュー

項目	説明
DNS サーバ	ホストと IP アドレスの対応を確認したり、修正したりするときに使用します。
DHCP サーバ	DHCP サーバの設定を行ったり、LAN 内の DHCP クライアントを確認するときに使用します。
ルーティング	ルーティングに関する設定を行うときに使用します。
ユーザ	管理者の設定の変更、および、本商品にアクセスを許可する PPTP クライアントの設定などを行うときに使用します。
日付と時刻	本商品の日付と時刻を変更するときに使用します。
ファームウェアアップデート	本商品のファームウェアをアップグレードするときに使用します。
IPSec	IPSec に関する設定を行うときに使用します。
UPnP	Universal Plug and Play に関する設定を行うときに使用します。
IPv6 ブリッジ	IPv6 サービスを利用するときに使用します。

PPPoE ブリッジ

ネットワークゲームやビデオチャットなど、ルータ配下で利用できないアプリケーションを利用するときに使用します。

システム設定

本商品のホスト名やドメイン名などを設定するときに使用します。

診断ツール

本商品から指定した IP アドレスへ Ping を行ない、通信テストするときに使用します。

設定情報の初期化

本商品の設定を購入時の状態に戻すときに使用します。

設定情報の保存/読み込み

設定変更する前など、設定情報を保存するとき、また保存した設定情報を読み込むときに使用します。

再起動

本商品を再起動するときに使用します。

ファームウェア情報

ファームウェアのバージョンを確認するときに使用します。

■［接続状況］アイコン

本商品の稼働時間やネットワーク情報などを確認するときに使用します。
クリックすると、［接続状況］画面に切り替わります。

■［オプション設定］アイコン

本商品にオプション機器を接続して利用する際に必要な設定を行います。

■［ログアウト］アイコン

クリックすると設定画面からログアウトします。

WAN 側の設定

ここでは、[PPPoE 接続]、または［PPPoE 以外の接続］を使用してインターネットに接続する方法について説明します。
設定方法は各接続により異なります。
お使いの接続方法をご確認のうえ、該当するページをご参照ください。

■ [PPPoE 接続] を設定する

1.プロバイダから IP アドレスを自動取得する場合、またはプロバイダからの情報をもとに IP アドレスを固定で設定する場合
→本商品の取扱説明書「第 4 章 インターネットへの接続」をご参照ください。

2.IP アドレスを固定で設定し、Unnumbered 接続する場合
→ P.6-11「PPPoE 接続で Unnumbered 接続を設定するとき」へお進みください。

3.PPPoE 接続を複数設定し、マルチセッション接続する場合
→ P.6-19「PPPoE 接続でマルチセッション接続を設定するとき」へお進みください。

■ [PPPoE 以外の接続] を使用する

1.PPPoE 接続を行なわず、DHCP などによりプロバイダから IP アドレスを自動取得する場合
→ P.6-32「PPPoE 以外の接続で自動取得を設定するとき」へお進みください。

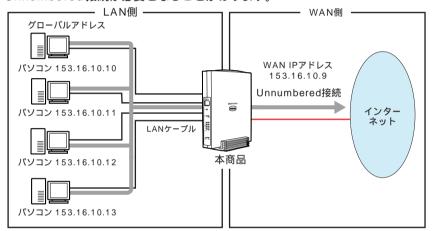
2.プロバイダからの情報をもとに、IP アドレスを固定で設定する場合
→ P.6-36「PPPoE 以外の接続で固定 IP アドレスを設定するとき」へお進みください。

3.IP アドレスを固定で設定し、Unnumbered 接続する場合
→ P.6-38「PPPoE 以外の接続で Unnumbered 接続を設定するとき」へお進みください。

PPPoE接続を設定する

ここでは、本商品の取扱説明書で説明していないPPPoE接続を使用した設定方法について説明します。

PPPoE接続でUnnumbered接続を設定するとき

本商品のPPPoE接続で、Unnumbered接続する方法について説明します。
プロバイダとの契約で複数の固定IPアドレスを取得している場合には、Unnumbered接続が必要となることがあります。

本商品でUnnumbered接続の設定を行なう場合、以下の手順になります。

1.WAN PPPoEの設定
2.パソコンのIPアドレスの設定

! ご注意

- プロバイダからの設定資料をご用意ください。
- Unnumbered接続の設定を行なう前に、簡単設定ウィザードでPPPoE接続を作成してください。

→本商品の取扱説明書「第4章 インターネットへの接続」をご参照ください。

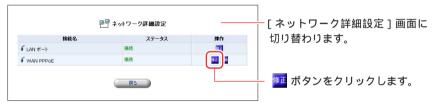
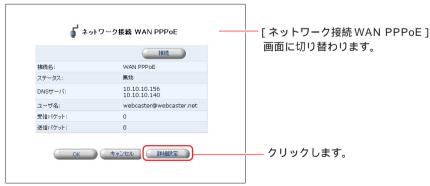
プロバイダから複数のグローバルIPアドレスが割り当てられる場合、1つのサブネットとして連続したグローバルIPアドレスが割り当てられます。このうち最初（ネットワークアドレス）と最後（ブロードキャストアドレス）はシステムで予約されており、ホスト（コンピュータやサーバ）には使用できません。

例）プロバイダから153.16.10.8～153.16.10.15の8個のグローバルIPアドレスが割り当てられた場合

153.16.10. 8	ネットワークアドレス（使用不可）
153.16.10. 9	ルータ用（WAN PPPoEポート）
153.16.10.10 ～ 153.16.10.14	ホスト用
153.16.10.15	ブロードキャストアドレス（使用不可）

WAN PPPoE の設定

1　サイドバーの［ネットワーク詳細設定］アイコンをクリックします。

2　すでに設定してある［WAN PPPoE］接続の「修正」ボタンをクリックします。

3　回線が接続されている場合は、［切断］ボタンをクリックし、回線をいったん切断します。
［詳細設定］ボタンをクリックします。

4 ［IP 設定］欄から、［IP アドレスを固定設定する］を選択します。

5 プロバイダからの情報をもとに IP アドレスを入力します。

6 ［DNS サーバ］欄から［DNS サーバアドレスを固定設定する］を選択し、DNS サーバアドレスを入力します。

入力します。

7 ［LAN 側グローバルネットワーク］欄の［ネットワークアドレス］にプロバイダから割り当てられたネットワークアドレスとサブネットマスクを入力します。

［OK］ボタンをクリックします。

入力します。

クリックします。

これで本商品の［WAN PPPoE］側の設定は終了しました。
次にお使いのパソコンにグローバル IP アドレスを設定します。

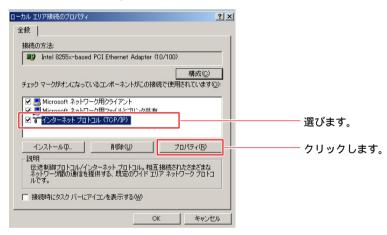
パソコンのIPアドレス設定

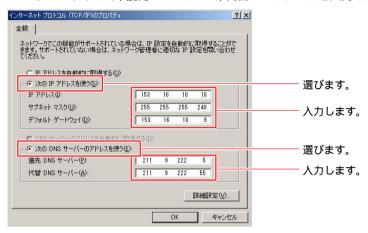
ここでは、Windows® 2000を例にして、パソコンにグローバルIPアドレスを設定する方法について説明します。
他のOSをお使いのお客さまは、**P.8-2「第8章 パソコンのIPアドレスの管理」をご参照ください。**

1 **[スタート] - [設定] - [コントロールパネル] をクリックします。**

2 **[ネットワークとダイアルアップ接続] をダブルクリックします。**

3 [ローカルエリア接続] アイコンを右クリックし、[プロパティ] を選択します。

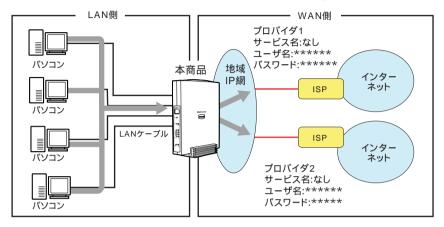
4 [インターネットプロトコル(TCP/IP)] を選択し、[プロパティ] ボタンをクリックします。

5 [次のIPアドレスを使う]と[次のDNSサーバのアドレスを使う]にチェックを付けます。

プロバイダからの情報をもとに、IPアドレス、サブネットマスク、デフォルトゲートウェイ、優先DNSサーバ、代替DNSサーバを入力します。

※プロバイダからの設定資料にそって設定してください。

6 [OK]ボタンをクリックします。

7 以上で設定は終了です。

PPPoE 接続でマルチセッション接続を設定するとき

本商品では、PPPoE マルチセッションに対応しております。
マルチセッション利用時は複数のプロバイダを登録し同時に接続することができ、最大 4 セッションの接続を同時に行うことができます。

また、複数の接続先を登録した場合は、デフォルトゲートウェイの変更や接続先の優先順位の変更を自由に行うことができます。
通常は PPPoE 接続を作成した順に登録され、優先順位が決まります。
IP アドレスを直接指定した通信は、メトリックが一番小さく設定された PPPoE セッションへ転送されます。ドメイン名、ホスト名を利用した通信は、プロキシ DNS を利用した通信が行われるため、この限りではありません。

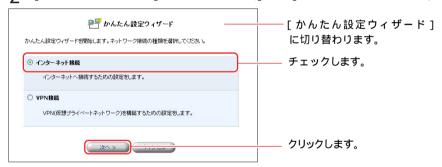
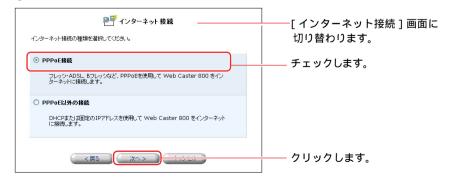
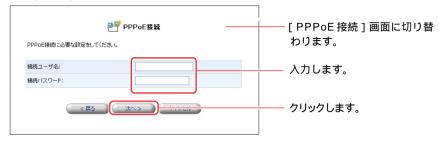
接続名	優先順位	メトリック
WAN PPPoE	1	20
WAN PPPoE2	2	21
WAN PPPoE3	3	22
WAN PPPoE4	4	23

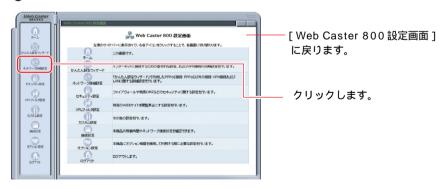
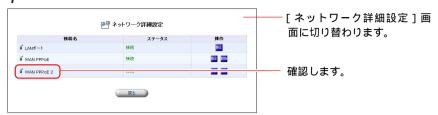
! ご注意

- 複数セッションへの接続機能は、複数の PPPoE セッションへの接続を同時に行えるサービス（マルチセッション）でのみご利用することができます。
  マルチセッションがサポートされていないサービスの場合は、複数セッションへの同時接続機能はご利用できません。
- Unnumbered 接続とは異なります。
- PPPoE 接続以外の接続（DHCP 接続など）ではこの機能は使用できません。

複数の接続先を登録する

1 **ここでは、1 つ目の PPPoE 接続が既に登録されていて、2 つ目を追加登録する場合について説明します。**
サイドバーの [かんたん設定ウィザード] アイコンをクリックします。

2 **[インターネット接続] にチェックをつけ、[次へ] ボタンをクリックします。**

3 **[PPPoE 接続] にチェックをつけ、[次へ] ボタンをクリックします。**

4　**2つ目のプロバイダから指定された接続ユーザ名、接続パスワードを入力します。**
[次へ]ボタンをクリックします。

5　**[設定完了]の画面が表示されますので、[完了]ボタンをクリックします。**

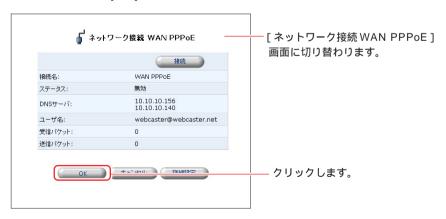
6　**サイドバーから[ネットワーク詳細設定]アイコンをクリックします。**

7　2 つ目の［WAN PPPoE2］が表示されていることを確認します。

8　以上で設定は終了です。

3 つ目、4 つ目の PPPoE の接続先を登録する場合は、同様の手順でお進めください。

PPPoE 接続の削除

1 **サイドバーの［ネットワーク詳細設定］アイコンをクリックします。**

2 **［接続名］欄から削除する PPPoE 接続の［修正］ボタンをクリックします。**

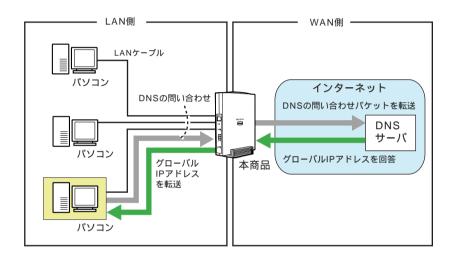
3 **回線が接続されてる場合は、［切断］ボタンをクリックし、回線をいったん切断します。［OK］ボタンをクリックします。**

4 **[接続名]欄から削除するPPPoE接続の[削除]ボタンをクリックします。[削除]ボタンは続けてクリックせずに、1回のみクリックしてください。**

※なお、本商品の設定画面が応答しなくなった場合は、いったん本商品の電源を入れ直し、再起動してください。

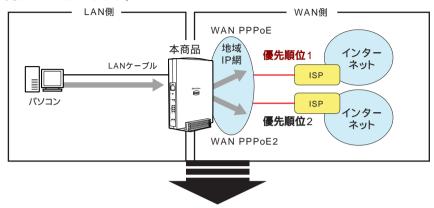
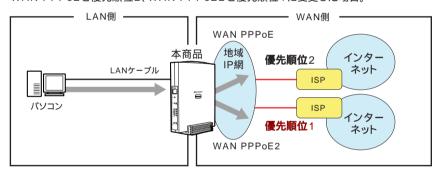
5 **[戻る]ボタンをクリックします。**

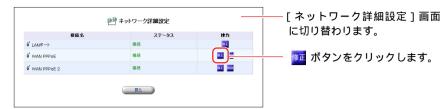
6 **以上で設定は終了です。**

プロキシ DNS

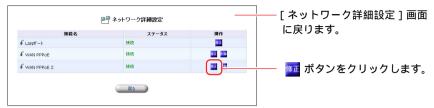
本商品には「プロキシ DNS」機能が搭載されています。プロキシ DNS とは、LAN 側の各パソコンからインターネット上のドメイン名を指定した接続（DNS の問い合わせ）があった場合に、それをインターネット上の DNS サーバにフォワーディングして、対応する IP アドレスを各パソコンに回答する機能です。
LAN 側のパソコンからは、インターネット上の DNS サーバに代理で問い合わせていることはわからず、単に、本商品がインターネット上のドメインと各 IP アドレスの対応を管理する DNS サーバとして動作しているように見えます。

WAN 側で複数セッションを接続している時には、LAN 側のパソコンから DNS の問い合わせがあった場合、本商品のプロキシ DNS 機能は、全てのセッション上の DNS サーバに問い合わせのパケットを送信します。この場合、返答のあった DNS サーバのセッションに対して通信が行われるようルーティングテーブルを動的に変更し通信を行います。2 つ以上のセッションの DNS サーバから返答があった場合は、先に返答があった方のセッションを使用します。

接続先の優先順位を変更する

本商品で複数の接続先を登録した場合、登録した順に優先順位が設定されます。本商品はPPPoE接続を設定後、デフォルトゲートウェイの変更や優先順位を変更することができます。

WAN PPPoEを優先順位2、WAN PPPoE2を優先順位1に変更した場合。

1　サイドバーから「ネットワーク詳細設定」アイコンをクリックします。

2 「接続名」欄から「WAN PPPoE」の［修正］ボタンをクリックします。

3 回線が接続されてる場合は、［切断］ボタンをクリックし回線をいったん切断します。［詳細設定］ボタンをクリックします。

4 ［デバイスメトリック］欄に「21」を入力し、[OK]ボタンをクリックします。

5 [OK]ボタンをクリックし、[ネットワーク詳細設定]の画面に戻ります。「接続名」欄から「WAN PPPoE2」の修正ボタンをクリックします。

6 回線が接続されてる場合は、［切断］ボタンをクリックし回線をいったん切断します。［詳細設定］ボタンをクリックします。

7 ［デバイスメトリック］欄に「20」を入力し、[OK]ボタンをクリックします。

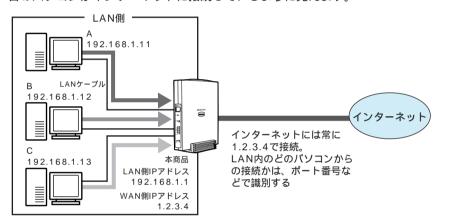
8 以上で設定は終了です。

本商品に設定されたWAN　PPPoE2がデフォルトゲートウェイ、WAN PPPoEが優先順位2に変更されました。

3つ目、4つ目のPPPoE接続の優先順位を変更する場合は、同様の手順でお進めください。

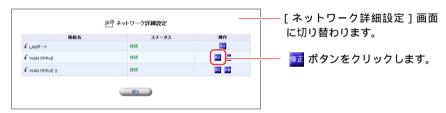
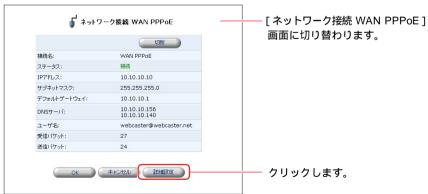
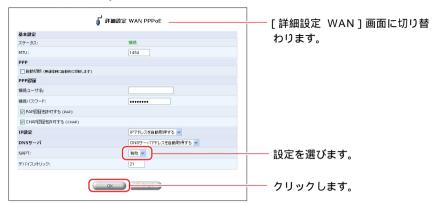
NAPT（IP マスカレード）

本商品では、ルーティングのモードとしてNAPTに対応しています。

複数のプライベートIPアドレスを1つのグローバルIPアドレスに変換する機能で、IPマスカレードとも呼ばれます。LAN側にプライベートIPアドレスを割り当てたパソコンが複数台あり、1つのグローバルIPアドレスでインターネットに接続する運用形態のときは、NAPTを使用します。
NAPTを使用した場合、LAN内で割り当てられてる複数のプライベートIPアドレスが、インターネットへの接続時に1つのグローバルIPアドレスに変換されます。さらに、ポート番号も変換されます。インターネット側からは、常に1台のパソコンがインターネットに接続しているように見えます。

※NAPT機能は、各WAN側のセッション毎に有効/無効の切り替えができます。これにより、NAPT無しのルータとしての機能を実現できます。

NAPTの設定を変更する

1 **サイドバーの[ネットワーク設定]アイコンをクリックします。**

2 **「接続名」欄から「WAN PPPoE」の［修正］ボタンをクリックします。**

3 **回線が接続されてる場合は、［切断］ボタンをクリックし回線をいったん切断します。［詳細設定］ボタンをクリックします。**

4 **[NAPT]欄のプルダウンメニューから有効/無効を選びます。[OK]をクリックします。**

5 **［ネットワーク接続］画面に戻ります。[OK]をクリックします。**

6 **以上で設定は終了です。**

PPPoE 以外の接続設定

**ここでは、PPPoE 以外の接続を使用した設定方法について説明します。
PPPoE 以外の接続サービスは、通常接続や DHCP によるアドレス自動設定、固定 IP アドレスの設定などがあります。**

PPPoE 以外の接続で自動取得を設定するとき

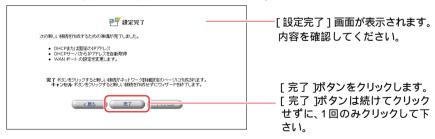
ここでは、[かんたん設定ウィザード] を使って IP アドレスを自動取得で設定する場合について説明します。

1 **サイドバーから [かんたん設定ウィザード] アイコンをクリックすると、ウィザードが開始されます。画面の指示に従って設定を進めてください。**

2 **[インターネット接続] にチェックをつけ、[次へ] ボタンをクリックします。**

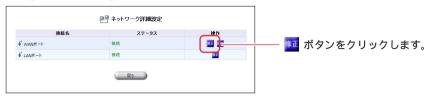
3 ［PPPoE 以外の接続］にチェックをつけ、［次へ］ボタンをクリックします。

4 ［自動取得］にチェックをつけ、［次へ］ボタンをクリックします。これでプロバイダからIP アドレスを自動的に取得することができます。

5 ［完了］ボタンをクリックします。設定を修正する場合は［戻る］ボタンをクリックし、修正する画面まで戻ってください。

6 **プロバイダからDNSサーバのIPアドレスが指定されている場合は、さらにその設定を行う必要があります。サイドバーから［ネットワーク詳細設定］アイコンをクリックします。**
［WANポート］の「修正」ボタンをクリックします。

修正 ボタンをクリックします。

7 **回線が接続されている場合は［無効］ボタンをクリックし、回線をいったん切断します。**
［詳細設定］ボタンをクリックします。

［ネットワーク接続　WANポート］画面が表示されます。内容を確認してください。

クリックします。

8 **［DNSサーバ］欄から［DNSサーバアドレスを固定設定する］を選択し、プロバイダからの情報をもとにDNSサーバアドレスを入力します。**

［詳細設定　WAN　ポート］画面に切り替わるので、DNSサーバの設定を行います。

選択します。

入力します。

※プロバイダの資料に従って設定してください。

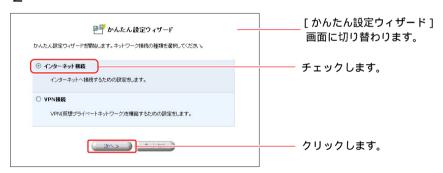
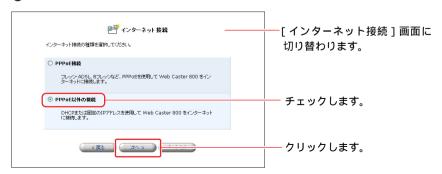
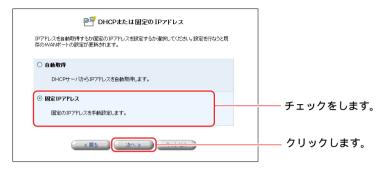
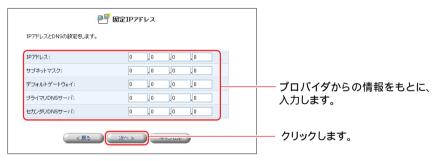
9 [OK] ボタンをクリックします。

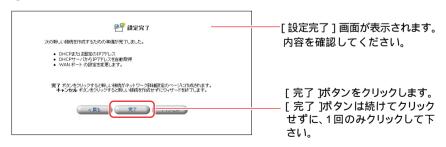
10 以上で設定は終了です。

PPPoE 以外の接続で固定 IP アドレスを設定するとき

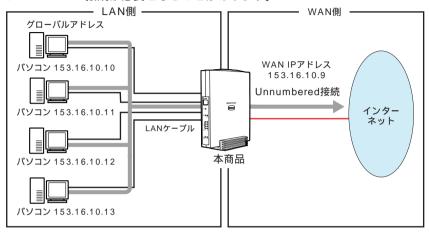
ここでは、[かんたん設定ウィザード] を使って固定 IP アドレスを設定するときの方法について説明します。

1　［かんたん設定ウィザード］アイコンをクリックすると、ウィザードが開始されます。画面の指示に従って進めてください。

2　［インターネット接続］にチェックをつけ、［次へ］ボタンをクリックします。

3　［PPPoE 以外の接続］にチェックをつけ、［次へ］ボタンをクリックします。

4 ［固定IPアドレス］にチェックをつけ、［次へ］ボタンをクリックします。

5 プロバイダからの情報をもとにIPアドレス、サブネットマスク、デフォルトゲートウェイ、DNSサーバのアドレスを入力し、［次へ］ボタンをクリックします。

※プロバイダの資料に従って設定してください。

6 ［完了］ボタンをクリックします。

7 以上で設定は終了です。

PPPoE 以外の接続で Unnumbered 接続を設定するとき

本商品の PPPoE 以外の接続で、Unnumbered接続する方法について説明します。プロバイダとの契約で複数の固定 IP アドレスを取得している場合には、Unnumbered 接続が必要となることがあります。

本商品で Unnumbered 接続の設定を行なう場合、以下の手順になります。

1.WAN ポートの設定
2.パソコンの IP アドレスの設定

ご注意

・プロバイダからの設定資料をご用意ください

プロバイダから複数のグローバルIPアドレスが割り当てられる場合、1つのサブネットとして連続したグローバルIPアドレスが割り当てられます。このうち最初（ネットワークアドレス）と最後（ブロードキャストアドレス）はシステムで予約されており、ホスト（コンピュータやサーバ）には使用できません。

例）プロバイダから153.16.10.8～153.16.10.15の8個のグローバルIPアドレスが割り当てられた場合

153.16.10. 8	ネットワークアドレス（使用不可）
153.16.10. 9	ゲートウェイ
153.16.10.10	ルータ用（WAN PPPoEポート）
～	ホスト用
153.16.10.14	
153.16.10.15	ブロードキャストアドレス（使用不可）

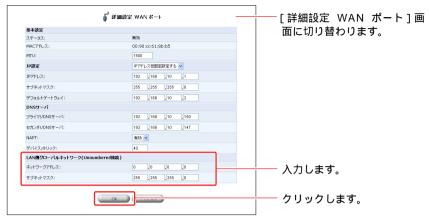
WAN ポートの設定

ここでは、PPPoE 以外の接続で固定 IP アドレスの接続がすでに登録されている場合について説明します。
本商品で固定 IP アドレスの接続を設定する場合は、P.6-36「PPPoE 以外の接続で固定 IP アドレスを設定するとき」へお進みください。

1　サイドバーの［ネットワーク詳細設定］アイコンをクリックします。

2　［WAN ポート］の修正ボタンをクリックします。

3　回線が接続されている場合は、［無効］ボタンをクリックし、回線をいったん切断します。［詳細設定］ボタンをクリックします。

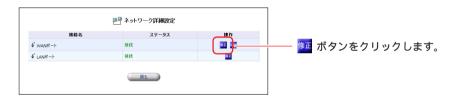
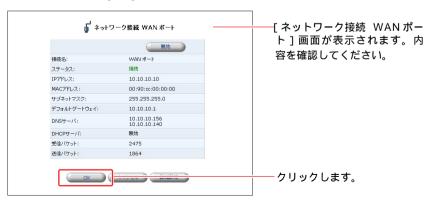
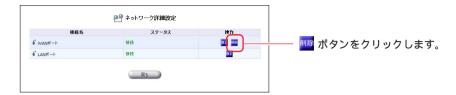
4 **「LAN側グローバルネットワーク」にプロバイダから割り当てられたネットワークアドレスとサブネットマスクを入力します。**
［OK］ボタンをクリックします。

5 **［OK］ボタンをクリックします。**

これで、本商品の［WANポート］側の設定は終了しました。
次にお使いのパソコンにグローバルIPアドレスを設定します。
P.6-16［パソコンのIPアドレス設定］へお進みください。

PPPoE 以外の接続の削除

ここでは、既に登録してあるPPPoE以外の接続を削除する場合について説明します。

1 サイドバーから[ネットワーク詳細設定]アイコンをクリックします。

2 [接続名]欄から削除するWANポート接続の[修正]ボタンをクリックします。

3 回線が接続されてる場合は、[無効]ボタンをクリックし、回線をいったん切断します。[OK]ボタンをクリックします。

4 **[接続名]欄から削除するWANポートの[削除]ボタンをクリックします。[削除]ボタンは続けてクリックせずに、1回のみクリックしてください。**

※なお、本商品の設定画面が応答しなくなった場合は、いったん本商品の電源を入れ直し、再起動してください。

5 **[戻る]ボタンをクリックします。**

6 **以上で設定は終了です。**

LAN 側の設定

ここでは、主に本商品の LAN 側の設定について解説します。

IP アドレスの設定

本商品の LAN 側ポートの IP アドレスを確認・変更する方法を解説します。

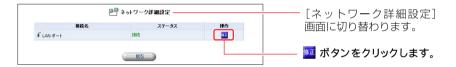
! ご注意

本商品の IP アドレスを変更する場合は、誤った IP アドレスを設定することのないようご注意ください。誤った IP アドレスを設定すると、インターネットに接続できなくなるなどのトラブルになることがあります。

LAN 側ポートの IP アドレスを確認・変更する

購入時の状態では、本商品の LAN 側ポートの IP アドレスは「192.168.1.1」が設定されています。
すでに LAN が構築されている環境に本商品を導入した場合などで、本商品の LAN 側ポートの IP アドレスを変更する必要があるときは、次の手順で行います。

1 **サイドバーから［ネットワーク詳細設定］アイコンをクリックします。**

2 **［LAN ポート］の、修正（修正）ボタンをクリックします。**

3 **［詳細設定］ボタンをクリックします。**

4　本商品のLAN側ポートのIPアドレスは「IP設定」欄に表示されます。IPアドレスを変更するときは、必要に応じて各項目を設定します。

5　画面の一番下にある［OK］ボタンをクリックし、［ネットワーク接続 LANポート］画面に戻ります。

※［OK］ボタンをクリックして［注意］画面に切り替わる場合には、その内容をご確認の上、さらに［OK］ボタンをクリックして［ネットワーク接続 LANポート］画面に戻ってください。

6　［OK］ボタンをクリックし、［ネットワーク詳細設定］画面に戻ります。

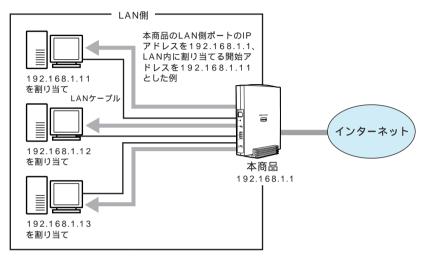
※Webブラウザで本商品のIPアドレスを指定して設定ページにアクセスしていた場合、続いて別の設定を行いたいときは、変更後のIPアドレスでアクセスし直してください。

MEMO

●**LAN側のIPアドレスを変更したとき**
LAN側のIPアドレスやサブネットマスクを変更したときは、変更後の内容に合わせて［DHCPサーバ］の設定も変更してください。

●**LAN内で起動しているパソコンがあるとき**
本商品のLAN側ポートのIPアドレスを変更するときに、LAN内で起動しているパソコンがある場合は、本商品のIPアドレスを変更した後でIPアドレスを再取得する必要があります。詳しくはP.8-2「パソコンのIPアドレスの管理」を参照してください。

DHCP サーバ設定

DHCP サーバ機能を利用すると、LAN 内のパソコンやネットワーク機器がLAN に接続されるたびに、他のどれとも重複しないIP アドレスを自動で割り当てることができます。

本商品の DHCP サーバ機能は、特定のパソコンに常に固定の IP アドレスを割り当てることもできます。
また固定の IP アドレスの割り当てと、動的な IP アドレスの割り当ての両方を設定することもできます。

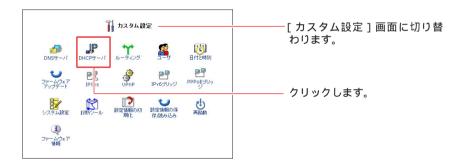
ご注意

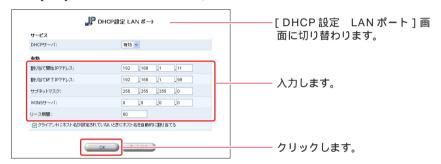
- 本商品の DHCP サーバ機能はデフォルトで有効になっています。
- DHCP サーバ機能を使用しないときは、LAN 側に接続されているパソコンすべてに、手動で IP アドレスを割り当ててください。パソコンの IP アドレス設定方法は P.8-2「パソコンの IP アドレスの管理」をご参照ください。
- パソコンに手動で IP アドレスを設定した場合、そのパソコンのホスト名や IP アドレスを本商品で管理することはできません。

DHCPサーバの基本設定

ここでは、DHCPサーバの基本的な設定について説明します

1　サイドバーから[カスタム設定]アイコンをクリックします。

2　[DHCPサーバ]アイコンをクリックします。

3 現在の DHCP サーバのサブネット、IP アドレスの割り当て範囲が表示されます。
設定を変更する場合は、[修正]ボタンをクリックします。

4 [DHCP 設定 LAN ポート]の画面が表示されます。
割り当てる IP アドレスの範囲、サブネットマスク、リース期間を設定し、[OK]ボタンをクリックします。

[DHCP サーバ]
　　DHCP サーバ機能の有効/無効を選択します。

[割り当て開始 IP アドレス]
　　割り当てる IP アドレスの、開始アドレスを入力します。

[割り当て終了 IP アドレス]
　　割り当てる IP アドレスの、終了アドレスを入力します。

[サブネットマスク]
　　割り当てるサブネットマスクを入力します。

[WINS サーバ]
　　WINS サーバを使用してる場合は、サーバアドレスを入力します。

[リース期間]
　　割り当てる IP アドレスの有効期限を分単位で入力します。

[クライアントにホスト名が設定されていないときにホスト名を自動的に割り当てる]
　　接続されているパソコンまたはネットワーク機器にホスト名が設定されていない場合自動的にホスト名が設定されます。

5 [OK]ボタンをクリックし、[DHCP サーバ]画面に戻ります。

6 以上で設定は終了です。

DHCP サーバから固定の IP アドレスを割り当てる

ここでは、特定のパソコンやネットワーク機器に DHCP サーバから常に固定の IP アドレスを割り当てる方法について説明します。

1　サイドバーから[カスタム設定]アイコンをクリックします。

2　[DHCP サーバ]アイコンをクリックします。

3 [DHCP 設定]ボタンをクリックします。

4 [固定 IP 割り当ての追加]欄から追加ボタンをクリックします。

5 追加したいパソコンやネットワーク機器のホスト名、IP アドレス、MAC アドレスを入力し、[OK]ボタンをクリックします。

[ホスト名]

パソコンまたはネットワーク機器のホスト名を入力します。半角英数字を使用し、1～63 文字の範囲で入力してください。

[IP アドレス]

パソコンまたはネットワーク機器に割り当てる IP アドレスを入力します。

[MAC アドレス]

IP アドレスを割り当てるパソコンまたはネットワーク機器の MAC アドレスを入力します。MAC アドレスの確認の方法は P.8-26「MAC アドレスの確認」をご参照ください。

6 追加したホストが[DHCP 設定]画面に表示されているのを確認します。

7 以上で設定は終了です。

IP アドレスの修正

ここでは、既に DHCP サーバから自動に IP アドレスが割り当てられているパソコンまたはネットワーク機器の設定を変更する方法について説明します。

1 **サイドバーから[カスタム設定]アイコンをクリックします。**

2 **[DHCP サーバ]アイコンをクリックします。**

3 [DHCP 設定]ボタンをクリックします。

4 設定を変更したいホストの[修正]ボタンをクリックします。

※パソコンにどのIP アドレスが割り当てられているかを調べる方法はP.8-2「IP アドレスの確認」をご参照ください。

5 [固定割り当て]にチェックを付け、[OK]ボタンをクリックします。

6 タイプが[固定]になっているのを確認し、ホストの[修正]ボタンをクリックします。

7 IP アドレスを固定で割り当てたり、ホスト名、MAC アドレスの修正を行うことができます。

8 [OK]ボタンをクリックし、[DHCP 設定]画面に戻ります。

9 以上で設定は終了です。

IP アドレスの削除

ここでは、登録済みのIP アドレスとホスト名の対応を削除する方法について説明します。

1　サイドバーから[カスタム設定]をクリックします。

2　[DHCP サーバ]をクリックします。

3 ［DHCP 設定］ボタンをクリックします。

4 削除したいホストの削除ボタンをクリックします。

5 ［戻る］ボタンをクリックし、［DHCP サーバ］画面に戻ります。

6 以上で設定は終了です。

DHCP サーバ機能の有効/無効を設定する

ここでは、DHCP サーバ機能の有効/無効を設定する方法について説明します。

1　サイドバーから[カスタム設定]をクリックします。

2　[DHCP サーバ]をクリックします。

3 **現在のDHCPサーバのサブネット、IPアドレスの割り当て範囲が表示されます。
設定を変更する場合は、[修正]ボタンをクリックします。**

4 **[DHCPサーバ]欄で[有効]を選択するとDHCPサーバ機能が有効になります。[無効]を選択するとDHCPサーバ機能が無効になります。**

ご注意

- **DHCPサーバ機能を無効にした場合は、本商品のLAN側に接続されてるパソコンまたはネットワーク機器に、手動でIPアドレスを設定してください。**

5 **[OK]ボタンをクリックし、[DHCPサーバ]画面に戻ります。**

※[OK]ボタンをクリックして［注意]画面に切り替わる場合には、その内容をご確認の上、さらに［OK］ボタンをクリックして［DHCPサーバ］画面に戻ってください。

6 **以上で設定は終了です。**

DNS サーバ設定

本商品の DNS サーバは、LAN 内のパソコンやネットワーク機器のホスト名と IP アドレスの対応を管理しています。

DNS サーバは DHCP サーバと同じ削除対応表を参照しています。DHCP サーバの設定時にホスト名を登録しておくと、他に特別な設定をせずに、ホスト名および対応する IP アドレスが DNS サーバで管理されます。

! ご注意

- 本商品の DNS サーバは、LAN 内のドメイン名と IP アドレスの対応だけを管理しています。
- インターネット上のドメイン名を指定した通信では、本商品の「プロキシ DNS」機能が使用されます。

DHCP サーバによるホスト名と IP アドレスの確認

本商品の DNS サーバは DHCP サーバと同じ対応表を参照しています。DHCP サーバでホスト名と IP アドレスを登録した場合は、DNS サーバにも反映されます。

ここでは、DHCP サーバ機能で自動登録されたホスト名と IP アドレスを確認します

1 **サイドバーから[カスタム設定]をクリックします。**

2 **[DHCP サーバ]をクリックします。**

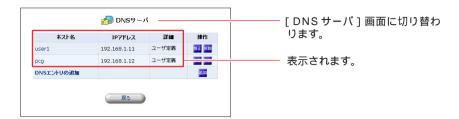
3 [DHCP 設定]ボタンをクリックします。

4 DHCP サーバ機能により、本商品に登録されてるホスト名とその IP アドレスが表示されます。

5 [戻る]ボタンをクリックし、[DHCP サーバ]画面に戻ります。

6 [OK]ボタンをクリックし、[カスタム設定]画面に戻ります。

7 [DNS サーバ]アイコンをクリックします。

8 **本商品のDNSサーバに登録されてるホスト名とIPアドレスが表示されます。**

9 **以上で確認は終了です。**

ホスト名とIPアドレスを手動で登録する

DHCPサーバ機能を使用しない場合は手動でホスト名とIPアドレスを登録する必要があります。

1　サイドバーから[カスタム設定]アイコンをクリックします。

2　[DNSサーバ]アイコンをクリックします。

3　**[DNS エントリの追加]から[追加]ボタンをクリックします。**

4　**DNS サーバに登録するホスト名と IP アドレスを入力し、[OK]ボタンをクリックします。**

5　**以上で設定は終了です。**

ホスト名とIP アドレスの修正

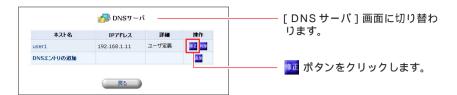
ホスト名やIP アドレスを変更したときは、DNS サーバに登録した情報も手動で変更する必要があります。

ご注意

- **DHCP サーバ機能を有効にしているときは、パソコンのホスト名は自動的にDNS サーバに反映されます。手動でホスト名を変更する必要はありません。**

1 **サイドバーから[カスタム設定]アイコンをクリックします。**

2 **[DNS サーバ]アイコンをクリックします。**

3　情報を修正したいホスト名の修正ボタンをクリックします

4　ホスト名とIP アドレスを修正し、[OK]ボタンをクリックします。

※ DHCP サーバによりIP アドレスを割り当てられたホストについては、ホスト名のみ修正が可能です。

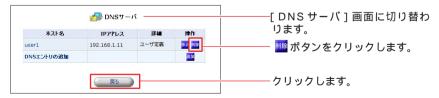
5　以上で設定は終了です。

ホスト名とIPアドレスの削除

登録されているホスト名とIPアドレスの削除を行います。

1 **サイドバーから[カスタム設定]アイコンをクリックします。**

2 **[DNSサーバ]アイコンをクリックします。**

3 **情報を削除したいホスト名の[削除]ボタンをクリックし、[戻る]ボタンをクリックします。**

4 **以上で設定は終了です。**

ルーティング設定

本商品は、ダイナミックルーティングのプロトコルとして RIP、RIP Version2 に対応しています。また、スタティックルーティングにも対応しています。

ダイナミックルーティングの設定

ここでは、ダイナミックルーティングを設定し、動的に経路情報を登録する方法について説明します。また、本商品は RIP、RIP Version2 に対応しています。

1 **サイドバーから[カスタム設定]アイコンをクリックします。**

2 **[ルーティング]アイコンをクリックします。**

3 **[ルーティングプロトコル]欄から[RIP −ルーティングプロトコル]にチェックを付けます。**

4 **[OK]ボタンをクリックします。**

5 **以上で設定は終了です。**

6

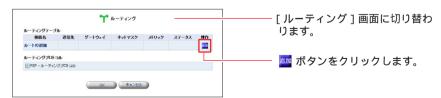
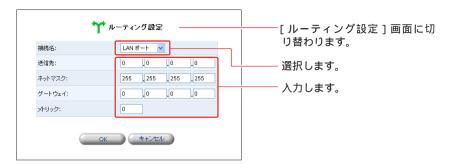
Web Caster 800の機能・設定の詳細

スタティックルーティングの経路情報を追加する

ここでは、経路情報を手動で設定する方法について説明します。

1　サイドバーから[カスタム設定]アイコンをクリックします。

2　[ルーティング]アイコンをクリックします。

3　[ルートの追加]から[追加]ボタンをクリックします。

4　経路情報を追加するデバイスを選択し、経路情報を入力します。

[接続名]
スタティックルーティングを設定する転送先のインタフェースを［LANポート］、［WANポート］、［WAN PPPoE］等から選択します。

[送信先]
パケットの送信先となるネットワークアドレスを入力します。

[ネットマスク]
パケットの送信先のネットマスクを入力します。

[ゲートウェイ]
宛先のネットワークに到達するための、最初のゲートウェイのアドレスを入力します。

[メトリック]
宛先のネットワークに到達するまでのホップカウント（経由するゲートウェイの数）を入力します。

5　[OK]ボタンをクリックします。

6　以上で設定は終了です。

! ご注意

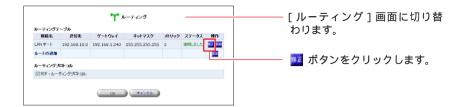
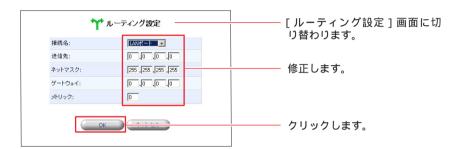
LAN→WANへのルーティングが可能なのは、LANポートに設定したネットワークからの通信のみです。他のネットワークからのパケットはルーティングできませんのでご注意下さい。

スタティックルーティングの経路情報を修正する

ここでは、既に設定したスタティックルーティングの経路情報を修正する方法について説明します。

1　サイドバーから[カスタム設定]アイコンクリックする。

2　[ルーティング]アイコンをクリックする。

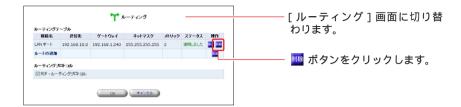
3 修正したい経路情報の[修正]ボタンをクリックします。

4 経路情報を修正し、[OK]ボタンをクリックします。

5 以上で設定は終了です。

スタティックルーティングの経路情報を削除する

ここでは、登録したスタティックルーティングを削除する方法について説明します。

1　サイドバーから[カスタム設定]アイコンクリックする。

2　[ルーティング]アイコンをクリックする。

3 **削除したい経路情報の[削除]ボタンをクリックします。**

4 **[OK]ボタンをクリックします。**

5 **以上で設定は終了です。**

UPnP設定

Universal Plug and Play（UPnP：ユニバーサルプラグアンドプレイ）は、ネットワークに接続するだけで、ネットワーク上の機器同士で簡単に通信できるようにする規格です。本商品は、UPnPに対応しており、次の機能を使用できます。

※購入時の設定でUPnPがONになっているため、特別な設定をする必要がありません。

- UPnPに対応しているOS（Windows® XPとWindows® Me）から、本商品を検出できます。
- UPnPに対応しているOS（Windows® XPとWindows® Me）から本商品の状態を確認したり、設定を一部変更できます。
- 本商品に接続されているLAN内のパソコンから、Windows® MessengerやMSN® Messengerなど、UPnPに対応しているアプリケーションを使用することができます。

なお、Windows® 98、Windows® 2000およびMacintosh® はUPnPに対応していません。したがって、UPnPの機能を使用することはできません。

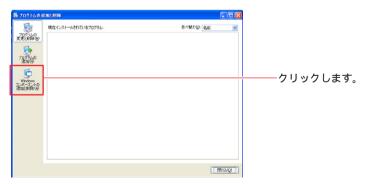
パソコンの UPnP の設定を確認する

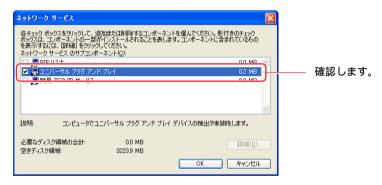
お使いのパソコンが、UPnP が使用できる状態になっているか確認してください。

■ Windows® XP の場合

1 **［スタート］ボタンをクリックし、［コントロールパネル］をクリックします。**

クリックします。

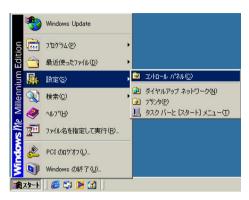
2 **［プログラムの追加と削除］ボタンをクリックし、画面左側にある［Windows コンポーネントの追加と削除］ボタンをクリックします。**

3 **［コンポーネント］欄から［ネットワークサービス］を選択し、［詳細］ボタンをクリックします。**

4 **ネットワークサービスの詳細が表示されますので、［ユニバーサルプラグアンドプレイ］の状態を確認します。**

［ユニバーサルプラグアンドプレイ］がチェックされているときは、パソコンがUPnPの機能が有効になっています。ダイアログを閉じてください。

チェックされていないときは、［ユニバーサルプラグアンドプレイ］が無効になっています。チェックを付け、［OK］ボタンをクリックします。画面の指示に従って、インストールを続けてください。

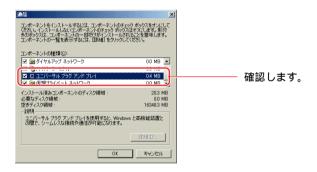
5 **以上で設定は終了です。**

■ Windows® Me の場合

1　［スタート］ボタンをクリックし、［設定］→［コントロールパネル］の順にクリックします。

2　［アプリケーションの追加と削除］ボタンをクリックします。［アプリケーションの追加と削除］ダイアログが表示されたら、［Windows ファイル］タブをクリックします。

クリックします。

3 **［コンポーネントの種類］欄から［通信］を選択し、［詳細］ボタンをクリックします。**

4 **通信の詳細が表示されますので、［ユニバーサルプラグアンドプレイ］の状態を確認します。**

5 **［ユニバーサルプラグアンドプレイ］がチェックされているときは、パソコンがUPnPの機能が有効になっています。ダイアログを閉じてください。**
チェックされていないときは、［ユニバーサルプラグアンドプレイ］が無効になっています。チェックを付け、［OK］ボタンをクリックします。画面の指示に従ってインストールを続けてください。

6 **以上で設定は終了です。**

本商品のUPnP機能をOFFにする

本商品でUPnP機能を使用しないときは、次のように操作します。

1　サイドバーの［カスタム設定］アイコンをクリックします。

2　［UPnP］アイコンをクリックします。

3　UPnPの機能をOFFにするときは、チェックボックスのチェックを外します。

4　［OK］ボタンをクリックします。

5　以上で設定は終了です。

UPnPセッション選択機能

ここでは、マルチセッション使用時のＵＰｎＰ適用セッションを設定する方法について説明します。本商品では、マルチセッション使用時に設定したセッション（最大4）のどれかに、UPnP機能を設定することができます。接続セッションが１つの場合は、本機能の設定は必要ありません。

本機能を設定する場合は、マルチセッションの接続設定を行う必要があります。
P.6-19「ＰＰＰｏＥ接続でマルチセッション接続を設定するとき」をご参照ください。なお、UPnP適用セッションは複数選択することができません。

1　サイドバーから［カスタム設定］アイコンをクリックします。

2　［カスタム設定］画面が表示されます。［UPnP］アイコンをクリックします。

3　［UPnP］の画面が表示されます。［UPnPを適用する接続］欄に現在接続済みのセッションが表示されます。

4 UPnP機能を利用するセッションを選択します。

! ご注意

本機能で設定した接続セッション以外でUPnP機能はご利用できません。

5 [OK] ボタンをクリックします。

6 以上で設定は終了です。

! ご注意

UPnP を適用する接続を変更した場合は、設定を変更後本商品を再起動してください。

セキュリティの設定

セキュリティ機能

インターネットに接続すると、LAN内のパソコンがインターネットからの攻撃を受けたり、不正なアクセスをされたりするという危険があります。そのため、LANを保護する十分なセキュリティ対策を行うことが、快適にインターネットを使う上で重要なポイントとなります。
本商品では、インターネットへの常時接続を行う上でのセキュリティ対策として次の機能を搭載しています。

NAPT（IPマスカレード）	プロバイダから取得したグローバルIPアドレスを、LAN内のプライベートIPアドレスに変換する機能により、インターネット側からLAN内のパソコンを特定できず、アクセスすることができません。このため、外部からの不正アクセスが困難になります。
ステートフル・パケット・インスペクション	ファイアウォール方式として、ステートフル・パケット・インスペクション方式を採用しています。通信セッションごとにパケットの整合性を確認し、必要なポートだけを開くようにします。通信が終了すると利用したポートを遮断します。 さらに、インターネット側からのDoS（Denial of Services）攻撃パターンを識別し、不正なアクセスを遮断することが可能です。
ALG（Application Level Gateway）	アプリケーションレベルでパケットの通過・遮断を判断します。
パケットフィルタリング	インターネットから送られてきたパケットを検査して通過させるかどうかを判断する機能です。どのような条件でパケットを通過させるか、遮断するかをプロトコル/ポートごとに任意に設定できます。
DMZ	LAN内の1台のパソコンをDMZホストとすると、WAN側からの全ての接続要求がDMZホストに転送されるようになります。
ユーザー名・パスワードによるユーザ認証	本商品の設定を変更するには、ログイン名とログインパスワードが必要です。

セキュリティレベル設定

ここでは、本商品の基本的なセキュリティレベルの設定を行います。
セキュリティ対策を考える時は、実際のデータのやり取りの流れに合わせて「LANからインターネットへの通信」と「インターネットからLANへの通信」のそれぞれに対してルールを考える必要があります。
一般的には、LANからインターネットにはアクセスできるようにし、インターネットからLANにはアクセスを拒否するように設定します。

本商品のセキュリティ機能には3段階のレベルがあらかじめ用意されています。
さらに、用途に応じて設定をカスタマイズすることができます。

セキュリティレベル設定

1　サイドバーから［セキュリティ設定］アイコンをクリックします。

［セキュリティ設定］画面に切り替わります。

セキュリティの設定が3段階で用意されています。
購入時の設定では、［セキュリティレベル標準］が選択されています。

2 必要に応じて、レベルを変更します。

セキュリティレベル	インターネット側からの接続要求	LAN内のパソコンからの接続要求
最大	**拒否** インターネット側からLANにアクセスできません。ただし、[ローカルサーバ]と[リモートアクセス]画面で設定したサービスは使用できます。	**制限あり** LAN内のパソコンで、Webサービス、e-mailなどのよく使うインターネットのサービスのみ使用できます。※
標準	**拒否** インターネット側からLANにアクセスできません。ただし、[ローカルサーバ]と[リモートアクセス]画面で設定したサービスは使用できます。	**制限なし** LAN内のパソコンで、すべてのインターネットのサービスが使用できます。
最小	**制限なし** インターネットからLANへのアクセスをすべて許可します。	**制限なし** LAN内のパソコンで、すべてのインターネットのサービスが使用できます。

※[セキュリティレベル最大]を選択しているとき、LAN側のパソコンから使用できるインターネットのサービスは次のとおりです。
Telnet、FTP、HTTP、HTTPS、DNS、IMAP、POP3、SMTP、 Ping

! ご注意

[セキュリティレベル最小]を選択すると、セキュリティ機能が一切適用されなくなりますので、必要な場合にのみ設定してください。

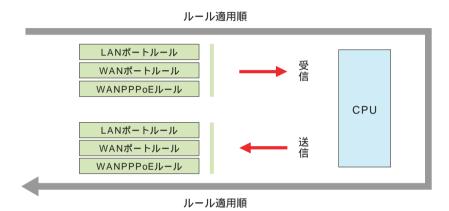
3 IP フラグメント化されたパケットを利用した攻撃を防ぐためには、[IP フラグメントパケットを遮断する] をチェックします。

※IPSec を利用する仮想プライベートネットワークや UDP をベースにしたサービスによっては、IP フラグメントを利用するものがあります。このようなサービスを利用するときは、チェックを外してください。

4 [OK] ボタンをクリックします。

選択したセキュリティレベルに変更されます。

パケットフィルタリング設定

本商品のパケットフィルタの機能は、本商品が受信したパケット、送信するパケットに対してあらかじめ設定してあるフィルタルールを適用します。
フィルタルールには、[LAN ポートルール]、[WAN ポートルール]、[WAN PPPoE ルール]があります。

パケットフィルタの新規設定

ここでは、本商品にパケットフィルタを設定する方法について説明します。

1　サイドバーから[セキュリティ設定]アイコンをクリックします。

2　[パケットフィルタ]ボタンをクリックします。

3 [パケットフィルタ]画面が表示されます。

4 [受信パケット]欄、または[送信パケット]欄からルールを作成するインタフェースをクリックします。

※ここでは、例として[WAN PPPoE ルール]を選択します。他のインタフェースを選択した場合は同様の手順で設定してください。

本商品で設定できるルール一覧

[LANポートルール]
　LANポートのポートに対して適用されるルールになります。

[WANポートルール]
　WANのポートに対して適用されるルールになります。

[WAN PPPoEルール]
　WAN PPPoEのポートに対して適用されるルールになります。

[WAN PPTPルール]
　WAN PPTPのポートに対して適用されるルールになります。

5 [WAN PPPoEルール設定]画面が表示されます。[新規作成]欄から追加ボタンをクリックします。

［WAN　PPPoEルール設定］画面に切り替わります。

追加 ボタンをクリックします。

6 [フィルタルール追加]画面が表示されます。

［フィルタルールの追加］画面に切り替わります。

7 [IP アドレス]欄から送信元 IP アドレス、送信先 IP アドレスを入力します。

[すべて]を選択した場合は、全ての IP アドレスが対象になります。

[1 個を指定]を選択した場合は、指定した IP アドレスが対象になります。

[範囲指定]を選択した場合は、指定した IP アドレスの範囲が対象になります。

8 [動作]欄からフィルタの動作を選択します。

[破棄する]
パケットを破棄します。

[転送する]
このルールに合致するパケットと、このパケットに関わるセッションのパケットを通します。

[転送する(パケット)]
このルールに合致するパケットのみを通します。

6

Web Caster 800 の機能・設定の詳細

9 **［サービス名］欄に本商品に既に登録されているサービスやアプリケーションが表示されます。フィルタルールの対象となるサービスにチェックをつけます。登録されていないサービスを設定する場合は、P.6-103「新規にサービスを作成する場合」をご覧下さい。**

10 **［OK］ボタンをクリックします。**

※［OK］ボタンは画面の下の方にあります。スクロールして表示してください。

11 **複数のフィルタルールを作成する場合は、3～10の手順を繰り返します。**

12 **以上で設定は終了です。**

パケットフィルタの修正

1　サイドバーから[セキュリティ設定]アイコンをクリックします。

2　[パケットフィルタ]ボタンをクリックします。

3　**設定を変更したいインターフェースの修正ボタンをクリックします。**

※ここでは、例として[WAN PPPoE ルール]を選択します。他のインタフェースを選択した場合は同様の手順で設定してください。

4　**［WAN PPPoE ルール設定］の画面が表示されます。［修正］ボタンをクリックします。**

5 ［フィルタルールの編集］画面が表示されますので、必要な項目の修正を行い［OK］ボタンをクリックします。

※［OK］ボタンは画面の下の方にあります。スクロールして表示してください。

6 以上で修正は終了です。

パケットフィルタの削除

1 **サイドバーから[セキュリティ設定]アイコンをクリックします。**

2 **[パケットフィルタ]ボタンをクリックします。**

3　設定を削除したいインタフェースの[修正]ボタンをクリックします。

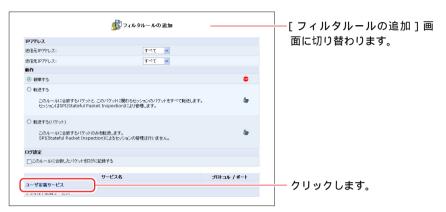
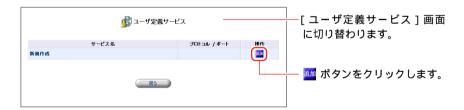
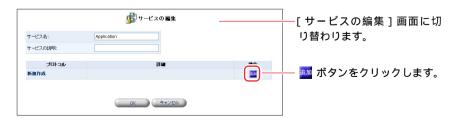
※ここでは、例として[WAN PPPoE ルール]を選択します。他のインタフェースを選択した場合は同様の手順で設定してください。

4　[WAN PPPoE ルール設定]の画面が表示されます。[削除]ボタンをクリックします。

5　以上で削除は終了です。

新規にサービスを作成する場合

ここでは、本商品にあらかじめ登録されていないサービスを設定する方法について説明します。

1 [フィルタルールの追加]画面から、[ユーザ定義サービス]をクリックします。

2 [ユーザ定義サービス]画面が表示されます。[追加]ボタンをクリックします。

3 [サービスの編集]画面が表示されます。[追加]ボタンをクリックします。

4　［プロトコル］欄から使用するプロトコルを選択します。

［プロトコル］
対象にするプロトコルをTCP、UDP、ICMP、GRE、ESP、AH、その他から選択します。

［送信元ポート/送信先ポート］
サービスやアプリケーションの発信元ポート/送信先ポート番号を入力します。
すべて　→全てのポートを指定します。
１個を指定　→１つのポート番号を指定します。
範囲指定　→ポート番号の範囲を指定します。

［ICMPメッセージ］
対象にするICMPメッセージを選択します。

［プロトコル番号］
対象にするプロトコル番号を入力します。

5　［OK］ボタンをクリックします。

6　［追加］ボタンをクリックすることで、複数のポートを指定することもできます。

7　全ての設定が終了しましたら［サービス名］に任意の名前を入力し、また［サービスの説明］欄に任意の説明を入力して、［OK］ボタンをクリックします。

8 [ユーザ定義サービス]の画面に戻ります。[サービス名]欄に作成したユーザ定義サービスが表示されるのを確認します。[戻る]ボタンをクリックします。

9 新規に作成したサービスが[ユーザ定義サービス]欄に表示されます。

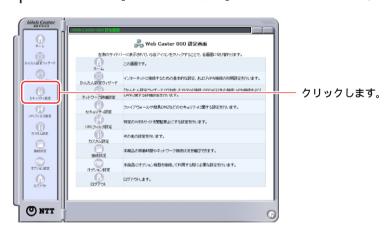
※フィルタルールの対象とするためには、新規に作成したサービスにチェックをつけて下さい。

10 以上で設定は終了です。

フィルタルールの例

ここでは、パケットフィルタの例としてNetBIOS関連で使われてるポート137～139のLANからWAN PPPoEへの通信を遮断する方法について説明します。Windows®のLANで使われてるNetBIOSのパケットにより、予期せぬインターネットへの通信が発生する場合があります。NetBIOS関連で使われてるポート137～139を遮断することで、予期せぬ通信を防ぎます。

方向	動作	プロトコル	送信元 IPアドレス	送信先 IPアドレス	送信元 ポート	送信先 ポート
受信パケット LANポート	破棄	TCP/UDP	すべて	すべて	すべて	137～139
送信パケット WAN PPPoE	破棄	TCP/UDP	すべて	すべて	すべて	137～139

1 サイドバーから[セキュリティ設定]アイコンをクリックします。

2 **[パケットフィルタ]ボタンをクリックします。**

3 **LAN側からWAN側へのNetBIOSのパケットを遮断するルールを作成します。**
[受信パケット]欄から[LANポートルール]の[修正]ボタンをクリックします。

4 [新規作成]欄から[追加]ボタンをクリックします。

5 送信元 IP アドレスに[すべて]、送信先 IP アドレスに[すべて]を選択します。

6 [動作]欄から[破棄する]にチェックを付けます。

7 [ユーザ定義サービス]をクリックします。

クリックします。

8 [ユーザ定義サービス]画面が表示されます。[新規作成]欄から[追加]ボタンをクリックします。

9 [サービスの編集]の画面が表示されます。[新規作成]欄から[追加]ボタンをクリックします。

10 プロトコルから[TCP]を選択します。送信元ポートに[すべて]、送信先ポートに[範囲指定]を選択し、ポート番号に137～139を入力します。

11 [OK]ボタンをクリックします。

12 同様にUDPポートも遮断しますので、[追加]ボタンをクリックします。

13 プロトコルから[UDP]を選択します。送信元ポートに[すべて]、送信先ポートに[範囲指定]を選択し、ポート番号に137～139を入力します。

14 [OK]ボタンをクリックします。

15 [サービスの編集]画面が表示されますので、サービス名に登録する名前を入力し、また[サービスの説明]欄に説明を入力して、[OK]ボタンをクリックします。

16 [ユーザ定義サービス]画面に戻ります。[サービス名]欄に作成したユーザ定義サービスが表示されるのを確認します。[戻る]ボタンをクリックします。

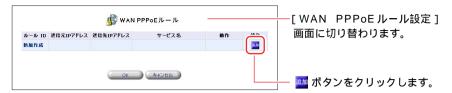
17 [ユーザ定義サービス]欄に作成したサービスが表示されますので、チェックを付け[OK]ボタンをクリックします。

※[OK]ボタンは画面の下の方にあります。スクロールして表示してください。

18 [OK]ボタンをクリックし、[パケットフィルタ]の画面に戻ります。

19 [OK]ボタンをクリックします。

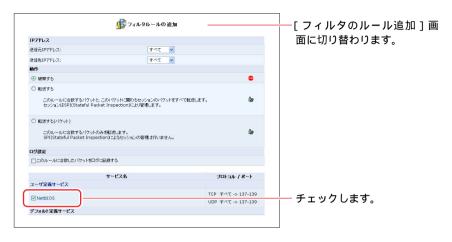
20 次に送信パケットの設定を行います。
[送信パケット]欄から[WAN PPPoE ルール]の[修正]ボタンをクリックします。

21 [新規作成]欄から[追加]ボタンをクリックします。

22 送信元IPアドレスに[すべて]、送信先IPアドレスに[すべて]を選択します。

23 [動作]欄から[破棄する]にチェックを付けます。

24 ［ユーザ定義サービス］欄に先ほど作成したサービスが表示されますので、チェックを付け、［OK］ボタンをクリックします。

［フィルタのルール追加］画面に切り替わります。

チェックします。

※［OK］ボタンは画面の下の方にあります。スクロールして表示してください。

25 ［OK］ボタンをクリックし、［パケットフィルタ］の画面に戻ります。

［WAN　PPPoE ルール設定］画面に切り替わります。

クリックします。

26 以上で設定は終了です。

リモートアクセス設定

リモートアクセス機能を使用することにより、インターネット側から本商品の各種サーバ機能にアクセスすることができます。
デフォルト設定では、不正アクセスから保護するためにリモートアクセスを許可していません。

お願い

不正アクセスにより本商品の設定を変更されないよう、通常はリモートアクセスを無効に設定しておき、必要な場合にのみ許可するようにしてください。

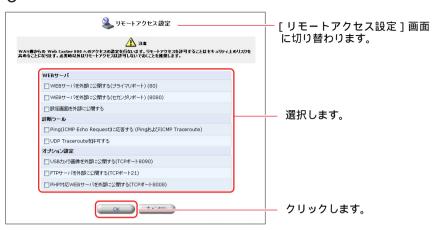
お知らせ

本商品に設定されたリモートアクセス機能は、ローカルサーバ、DMZホスト機能より優先されます。

リモートアクセスの設定

1 サイドバーから［セキュリティ設定］アイコンをクリックします。

2 ［リモートアクセス］ボタンをクリックします。

3 WAN側からのアクセスに関する設定を行います。

Webサーバ ※1	WEBサーバを外部に公開する（プライマリポート80）	本商品の設定画面またはWebサーバ、USBカメラ画面をWAN側に公開する場合選択します。TCPポート80番を使用します。※2
	WEBサーバを外部に公開する（セカンダリポート8080）	本商品の設定画面またはWebサーバ、USBカメラ画面をWAN側に公開する場合選択します。TCPポート8080番を使用します。※2
	設定画面を外部に公開する	本商品の設定画面を外部に公開する場合に選択します。 ※WAN側から設定画面にアクセスする場合のアドレスは「http://web caster 800のIPアドレス/setting/」になります。
診断ツール	Ping（IMCP Echo Requestに応答する（PingおよびICMP Traceroute）	Pingコマンドに返答する場合は選択します。
	UDP Tracerouteを許可する	tracerouteコマンドなどで、UDP上のルート確認をする場合は選択します。
オプション設定	USBカメラの画像を外部に公開する（TCPポート 8090）※3	本商品のオプションUSBカメラを接続し、カメラ画像を外部に公開する場合は、こちらを選択します。
	FTPサーバを外部に公開する（TCPポート 21）	本商品にUSBストレージを接続し、FTPサーバとしてWAN側に公開する場合は、こちらを選択します。
	PHP対応WEBサーバを外部に公開する（TCPポート 8008）※3	本商品のPHP対応サーバをWAN側に公開する場合選択します。TCPポート8008番を使用します。

※1　追加機能パッケージとして提供している「PHP対応WEBサーバ」とは異なります。

※2　USBカメラ画像をWAN側に公開するためには、更に[USBカメラ画像を外部に公開する(TCPポート 8090)を選択する必要があります。

※3　[USBカメラ画像を外部に公開する(TCPポート 8090)]および[PHP対応WEBサーバを外部に公開する(TCPポート 8008)]は、それぞれ追加機能パッケージ「USBカメラ」および「PHP対応WEBサーバ」をインストールして、パッケージを有効にした場合に表示されます。表示されない場合には、サイドバーの[オプション設定]－[機能追加パッケージ]をクリックして、それぞれのパッケージが有効になっているかご確認ください。

ワンポイント

Windows® からTracerouteコマンドを使用して、ルートの追跡を行う場合はPing[(ICMP Echo Requestに応答する(PingおよびICMP Traceroute)]をチェックしてください。

4 **[OK]ボタンをクリックします。**

5 **以上で設定は終了です。**

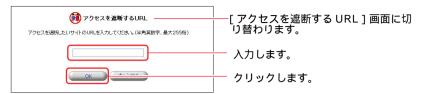
URL フィルタ設定

URL フィルタ機能を使うことで、LAN 側のパソコンから特定の Web サイトを閲覧できないように設定できます。
例えば、公序良俗に反するような Web サイトをあらかじめ本商品に設定しておくことで、LAN 側のパソコンからそのサイトの閲覧を禁止することができます。

URL フィルタの新規設定

1 **サイドバーから［URL フィルタ設定］アイコンをクリックします。**

2 **［新規作成］欄から［追加］ボタンをクリックします。**

3 閲覧を禁止したいWebサイトのURLまたはIPアドレスを入力し、[OK]ボタンをクリックします。

4 [WebサイトのURL]の一覧に設定したWebサイトが追加されます。

5 URLが追加されると、追加されたURLがインターネット上に存在するか自動的にチェックします。この間、[ステータス]欄には[確認中…]と表示されます。[表示の更新]ボタンをクリックして、入力されたURLが適切なものか確認します。

6 **入力されたURLに対して、インターネット上に存在することが確認できると[IPアドレス]欄にIPアドレスが表示され[ステータス]欄は[確認済み]に変わります。また、インターネット上に存在を確認できなかった場合は、[ステータス]欄に[IPアドレスが確認できません]と表示されます。**

［URLフィルタ設定］画面に切り替わります。

クリックします。

7 **[OK]ボタンをクリックすると、設定が有効になります。**

8 **以上で設定は終了です。**

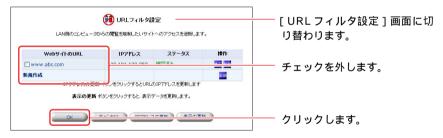
MEMO

ステータスに[IPアドレスが確認できません]が表示される場合

→Webブラウザを起動し設定したURLを入力し、Webブラウザに表示されるか確認してください。正しく表示されたときは、本商品に設定したURLが間違っている可能性があります。

URLフィルタの有効/無効の切替

1 **サイドバーから[URLフィルタ設定]アイコンをクリックします。**

2 **[WebサイトのURL]欄からURLフィルタを無効にしたいWebサイトのチェックを外し、[OK]ボタンをクリックします。**

3 **[ステータス]表示が[無効]に替わります。再度、URLフィルタを有効にする場合はチェックを付けます。**

4 **以上で設定は終了です。**

URLフィルタの修正

1　サイドバーから[URLフィルタ設定]アイコンをクリックします。

2　設定を変更したいWebサイトのURLの[修正]ボタンをクリックします。

3　[アクセスを遮断するURL]の画面が表示されましたら、新しいURLまたはIPアドレスを入力し、[OK]ボタンをクリックします。

4 ［Web サイトの URL］の一覧に変更した Web サイトが表示されます。

5 以上で設定は終了です。

URLフィルタの削除

1 **サイドバーから[URLフィルタ設定]アイコンをクリックします。**

2 **設定を削除したいWebサイトのURLの[削除]ボタンをクリックします。**

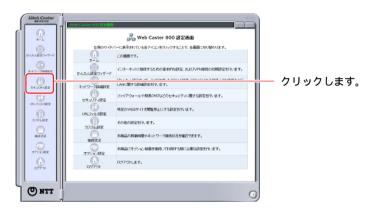
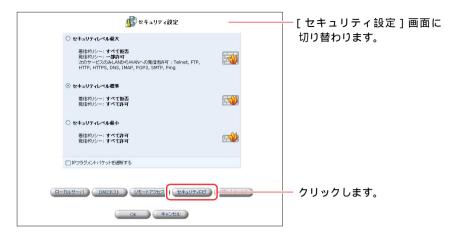
3 **[OK]ボタンをクリックします。**

4 **以上で設定は終了です。**

ログの管理

ここでは、LAN 側のパソコンからインターネットへの接続やインターネット側からLANへの接続、設定ページへのアクセスなどのログ情報を設定します。

セキュリティログの確認

1　サイドバーから[セキュリティ設定]アイコンをクリックします。

2 ［セキュリティログ］ボタンをクリックします。

3 ［セキュリティログ］画面が表示されます。現在のセキュリティに関するログが確認できます。

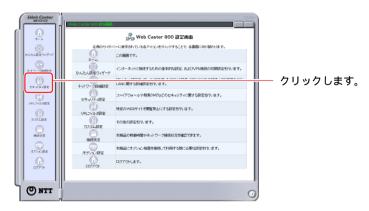
6 Web Caster 800の機能・設定の詳細

ログの見方（例）

イベント	種類	説明
Inbound/ Outbound Traffic	Connection accepted	接続要求がファイアウォールのセキュリティポリシーに適合していた場合に表示されます。
	Accepted - Host probed	ファイアウォールのセキュリティポリシーに適合したTCP接続要求があったが、インターネット側のホストが信頼できるかどうかわからない場合に表示されます。この場合、インターネット側のホストに認証が試みられます。 ※インターネット側からの接続要求に対してのみ表示されます。
	Accepted - Host trusted	認証を試みていたホストから応答があった場合に表示されます。 ※インターネット側からの接続要求に対してのみ表示されます。
	Accepted - Internal traffic	すべてのパケットがLAN側のホスト同士の間で自由に行き来できる場合に表示されます。
	Connection Refused- Policy violation	接続要求がファイアウォールのセキュリティポリシーに違反している場合に表示されます。
	Blocked - IP Fragment	ファイアウォールですべてのIPフラグメントをブロックする設定を行った場合で、IPフラグメントがブロックされたときに表示されます。エラーはブロックされたフラグメントごとに表示されます。
	Blocked - IP Source Routes	IPヘッダに始点経路制御オプションが設定されていることが原因で、パケットがブロックされたときに表示されます。
	Blocked - State-table error	ファイアウォールによってステートテーブル（LAN側のパソコンやネットワーク機器間のセッション状態に関する情報）が調査または操作されている間に、エラーがあった場合に表示されます。パケットはブロックされます。

Firewall Setup	Aborting configuration	ファイアウォールに関する設定がキャンセルされたときに表示されます。
	Configuration completed	ファイアウォールに関する設定が完了したときに表示されます。
	No IP for NAT	再設定中にIP アドレス無しのデバイスを検出したことを示しています。
WBM Login	Authentication Success	設定ページへのログインが成功したときに表示されます。
	Authentication Failure	設定ページへのログインが失敗したときに表示されます。
System Up/Down	The system is going DOWN for reboot	本商品を再起動するために終了したときに表示されます。
	The system is UP!	本商品が起動したときに表示されます。

ログのクリア

1　サイドバーから［セキュリティ設定］アイコンをクリックします。

2　［セキュリティログ］ボタンをクリックします。

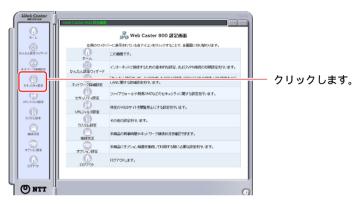
3 **[ログのクリア]ボタンをクリックすると、画面に表示されてるログが消去されます。**

4 **[戻る]ボタンをクリックします。**

5 **以上で設定は終了します。**

ログの詳細設定

ここでは、ログの保存に関する設定について説明します。

1 サイドバーから[セキュリティ設定]アイコンをクリックします。

2 [セキュリティログ]ボタンをクリックします。

3 [詳細設定]ボタンをクリックします。

4 [ログイベント]欄から保存するログ内容を選択します。

[許可した接続]

LAN側からインターネットへの接続、インターネット側からLANへの接続のうちファイアウォールの通過を許可されたものがログに保存されます。

[拒否した接続]

LAN側からインターネットへの接続、インターネット側からLANへの接続のうちファイアウォールの通過を拒否されたものがログに保存されます。

5　[設定]欄からログ容量が一杯になったときの設定を選択します。

[ログ容量が一杯になったらログを停止する]

ログを保存するメモリが一杯になったときにログの保存を停止する場合は、チェックします。
ログを保存するメモリが一杯になったとき古いログを消去し、続けてログを保存する場合はチェックを外します。

6　[OK]ボタンをクリックします。

7　以上で設定は終了します。

E-Mail通知機能の設定

本商品は、システムや回線、ファイアウォールに何かしらの異常が発生した場合電子メールで管理者に通知することができます。

E-Mail通知機能の設定

1　サイドバーから[カスタム設定]アイコンをクリックします。

2　[ユーザ]アイコンをクリックします。

3　E-mail通知機能を設定するユーザの[修正]ボタンをクリックします。

4　[E-mail アドレス]欄に、送信先の Mail アドレスを入力します。

5 ［システム通知レベル］欄から通知する内容を選択します。
システム通知は、システム情報に関するメッセージを送信します。

［エラー］

本商品が正しく動作していないなどの、致命的なエラーが発生した際にメッセージを送信します。

［警告］

注意を要するエラーが発生した際にメッセージを送信します。
警告を選択した場合は、エラーレベルのメッセージも送信されます。

［情報］

ユーザが本商品を利用したときに表示されるメッセージが送信されます。
情報を選択した場合は、エラーレベル、警告レベルのメッセージも送信されます。

6 [セキュリティ通知レベル]欄から通知する内容を選択します。

セキュリティ通知は、セキュリティログに表示されるメッセージを送信します。

[エラー]

重大なセキュリティイベントが発生した際に、メッセージを送信します。

[警告]

注意を要するセキュリティイベントが発生した際にメッセージを送信します。
警告を選択した場合は、エラーレベルのメッセージも送信されます。

[情報]

ユーザが本商品を利用したときに表示されるメッセージが送信されます。
情報を選択した場合は、エラーレベル、警告レベルのメッセージも送信されます。

7 本商品からメールを送信するための、SMTP メールサーバの設定をします。

[SMTP メールサーバの設定]をクリックします。

8 **［SMTP メールサーバ］欄にメールサーバのアドレスを入力します。また、［送信元メールアドレス］欄に、送信元のメールアドレスを入力します。**

9 **［OK］ボタンをクリックし、［ユーザ設定］画面に戻ります。**

10 **［OK］ボタンをクリックします。**

11 **以上で設定は終了です。**

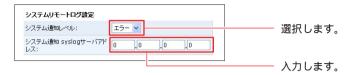
Syslogの設定

**本商品には、システムや回線、ファイアウォールに何かしらの異常が発生した場合Syslogサーバにログを送信することができます。
ここでは、ログをSyslogサーバに送信するための設定を説明します。**

Syslogの設定

1　サイドバーから[カスタム設定]アイコンをクリックします。

2　[システム設定]アイコンをクリックします。

3 ［システム通知レベル］欄から通知する内容を選択し、［システム通知Syslogサーバアドレス］にsyslogサーバのアドレスを入力します。

［エラー］
　システムに関する重大なメッセージを送信します。

［警告］
　システムに関する注意を要するメッセージを送信します。
　警告を選択した場合は、エラーレベルのメッセージも送信されます。

［情報］
　ユーザが本商品を利用したときに表示されるメッセージが送信されます。
　情報を選択した場合は、エラーレベル、警告レベルのメッセージも送信されます。

4 ［セキュリティ通知レベル］欄から通知する内容を選択し、［セキュリティ通知syslogサーバアドレス］にSyslogサーバのアドレスを入力します。セキュリティ通知は、セキュリティログに表示されるメッセージを送信します。

［エラー］
　重大なセキュリティイベントに関するメッセージを送信します。

［警告］
　注意を要するセキュリティイベントに関するメッセージを送信します。
　警告を選択した場合は、エラーレベルのメッセージも送信されます。

［情報］
　ユーザが本商品を利用したときに表示されるメッセージが送信されます。
　情報を選択した場合は、エラーレベル、警告レベルのメッセージも送信されます。

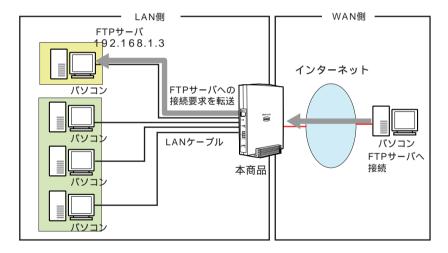
5 ［OK］ボタンをクリックします。

6 以上で設定は終了です。

サーバ公開設定

ここでは、外部にサーバを公開するときに必要な設定について説明します。

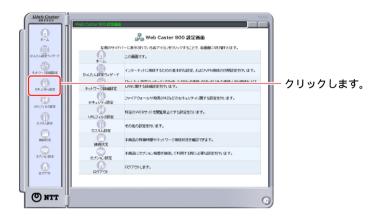
ローカルサーバ設定

LAN 側のサーバをインターネットに公開するときや、オンラインゲームやチャットなどのソフトウェアを使うときはローカルサーバ機能の設定を行います。
本商品には、あらかじめインターネットで使われるサービスやアプリケーションが登録されており、簡単に設定することができます。

ご注意

自動的にローカルサーバ設定が追加される場合がありますが、これは LAN 側に設置されたパソコンが UPnP により設定するものです。必要に応じて削除を行ってください。

ローカルサーバの設定

ここでは、ローカルサーバの詳細な設定を行います。

1　サイドバーから[セキュリティ設定]アイコンをクリックします。

2　[ローカルサーバ]ボタンをクリックします。

3 **[新規作成]欄から[追加]ボタンをクリックします。**

4 **[ローカルサーバの[追加]画面が表示されます。**
[ローカルホスト]欄にローカルサーバを設定するパソコンのホスト名またはIP アドレスを入力します。

6
Web Caster 800 の機能・設定の詳細

5　［デフォルト定義サービス］欄に本商品に既に登録されているサービスやアプリケーションが表示されます。インターネットに公開するサービスや、使用するアプリケーションを選択し、チェックします。

6　［OK］ボタンをクリックします。

※［OK］ボタンは画面の下の方にあります。スクロールして表示してください。

7　以上で設定は終了です。

ユーザ定義サービスの新規作成

ここでは、本商品にあらかじめ登録されていないサービスを設定し、ローカルサーバを利用する方法について説明します。

1　サイドバーから[セキュリティ設定]アイコンをクリックします。

2　[ローカルサーバ]ボタンをクリックします。

3 [新規作成]欄から[追加]ボタンをクリックします。

[ローカルサーバ]画面に切り替わります。

追加 ボタンをクリックします。

4 新規サービスを登録します。[ユーザ定義サービス]をクリックします。

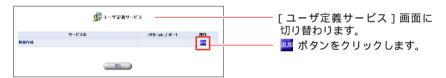
クリックします。

5 [ユーザ定義サービス]画面が表示されます。[新規作成]欄から[追加] ボタンをクリックします。

[ユーザ定義サービス]画面に切り替わります。

追加 ボタンをクリックします。

6 [サービスの編集]画面が表示されます。[新規作成]欄から[追加] ボタンをクリックします。

[サービスの編集]画面に切り替わります。

追加 ボタンをクリックします。

6 [プロトコル]欄から使用するプロトコルを選択し、ポート番号を入力します。

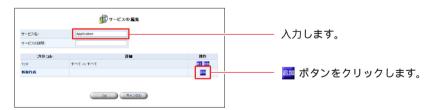
[プロトコル]
対象にするプロトコルをTCP、UDP、ICMP、GRE、ESP、AH、その他から選択します。その他を選択したときは、対象にするプロトコル番号を直接指定してください。

[発信元ポート/送信先ポート]
サービスやアプリケーションのポート番号を入力します。
すべて　　→全てのポートを指定します。
1個を指定→1つのポート番号を指定します。
範囲指定　→ポート番号の範囲を指定します。

[ICMPメッセージ]
対象にするICMPメッセージを選択します。

[プロトコル番号]
対象にするプロトコル番号を入力します。

7 [OK]ボタンをクリックします。

8 [追加]ボタンをクリックすることで、複数のポートを指定することもできます。

9 全ての設定が終了しましたら、[サービス名]欄に任意の名前を入力し、また[サービスの説明]欄に説明を入力して、[OK]ボタンをクリックします。

10 [ユーザー定義サービス]の画面に戻ります。

[サービス名]欄に作成したユーザ定義サービスが表示されていることを確認します。[戻る]ボタンをクリックします。

11 [ローカルサーバの追加]の画面に戻ります。

[ユーザ定義サービス]欄に作成したユーザ定義サービスが表示されていることを確認し、チェックします。

12 ローカルサーバ機能を使用するパソコンの設定を行います。

[ローカルホスト]欄にローカルサーバ機能を使用するパソコンのホスト名またはIP アドレスを入力します。

13 [OK]ボタンをクリックします。

※[OK]ボタンは画面の下の方にあります。スクロールして表示させてください。

14 **[ローカルサーバ]の画面に戻ります。ローカルサーバで使用するサービスとパソコンのIPアドレスが表示されます。**

15 **[OK]ボタンをクリックします。**

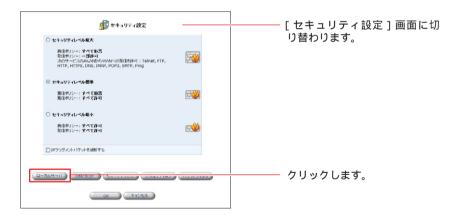
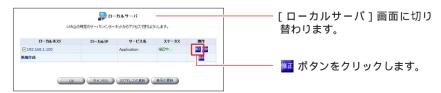
16 **以上で設定は終了です。**

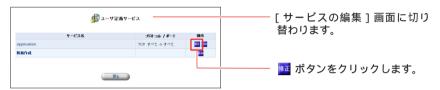
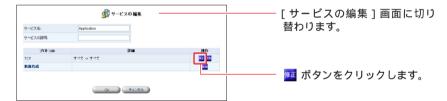
ユーザ定義サービスの修正

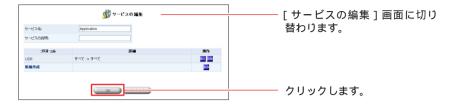
ここでは、既に作成したユーザ定義サービスを修正する方法について説明します。

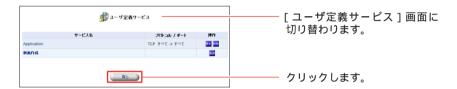
1　サイドバーから[セキュリティ設定]アイコンをクリックします。

クリックします。

2　[ローカルサーバ]ボタンをクリックします。

3　設定を変更するパソコンの[修正]ボタンをクリックします。

4 [ローカルサーバの編集]画面が表示されます。[ユーザー定義サービス]をクリックします。

5 [ユーザ定義サービス]の画面が表示されます。設定を変更したいサービスの[修正]ボタンをクリックします。

6 [サービスの編集]の画面が表示されます。設定を変更したいプロトコルの修正ボタンをクリックします。

7 [サービスの編集]の画面が表示されます。設定を変更したい項目を修正し、[OK]ボタンをクリックします。

6
Web Caster 800の機能・設定の詳細

8 [OK]ボタンをクリックします。

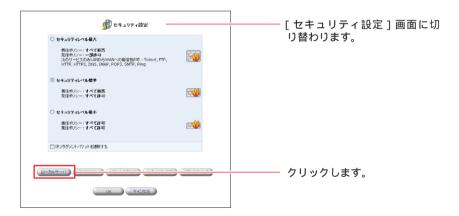
9 [ユーザ定義サービス]画面に戻ります。[戻る]ボタンをクリックします。

10 以上で設定は終了です。

ユーザ定義サービスの削除

1　サイドバーから[セキュリティ設定]アイコンをクリックします。

2　[ローカルサーバ]ボタンをクリックします。

6

Web Caster 800 の機能・設定の詳細

3 [新規作成]欄から[追加]ボタンをクリックします。

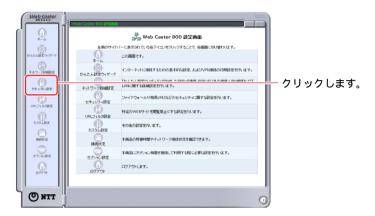
4 [ユーザ定義サービス]をクリックします。

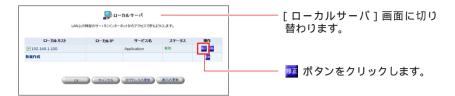
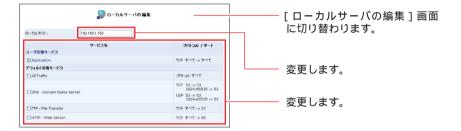
5 [ユーザ定義サービス]の画面が表示されます。削除したいサービスの削除ボタンをクリックします。

6 [戻る]ボタンをクリックします。

7 以上で設定は終了です。

ローカルサーバの修正

1 **サイドバーから［セキュリティ設定］アイコンをクリックします。**

2 **［ローカルサーバ］ボタンをクリックします。**

3　設定を変更したいパソコンの修正ボタンをクリックします。

4　［ローカルサーバーの編集］画面が表示されます。
使用するサービスまたはパソコンのホスト名またはローカルIPを変更できます。

5　［OK］ボタンをクリックします。

6　以上で設定は終了です。

ローカルサーバの有効/無効の切替

1 サイドバーから［セキュリティ設定］アイコンをクリックします。

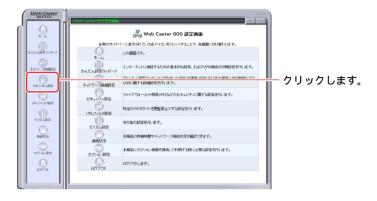
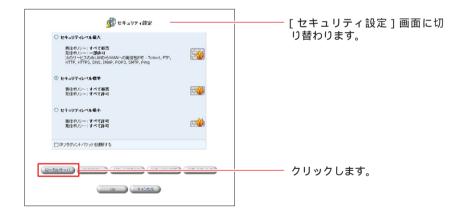
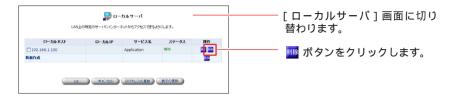
2 ［ローカルサーバ］ボタンをクリックします。

3 ［ローカルホスト］欄からサービスを無効にしたいローカルホストのチェックを外します。

4 ［OK］ボタンをクリックします。

5 以上で設定は終了です。

ローカルサーバの削除

1　サイドバーから[セキュリティ設定]アイコンをクリックします。

2　[ローカルサーバ]ボタンをクリックします。

3　**設定を削除したいローカルホストの[削除]ボタンをクリックします。**

4　**[OK]ボタンをクリックします。**

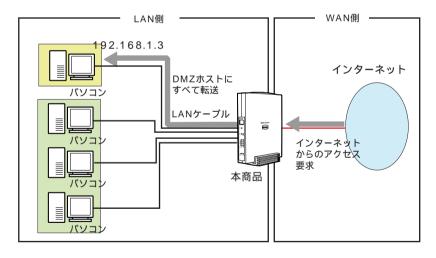
5　**以上で設定は終了です。**

DMZ ホストの設定

DMZ ホスト機能を使用すると、LAN 側にある 1 台のパソコンをインターネット上に公開できます。次のようなときに、DMZ ホストを指定します。

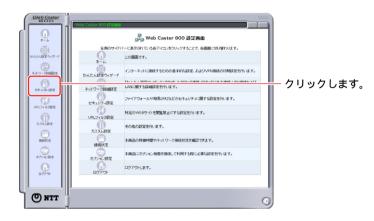
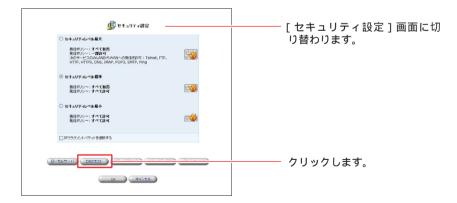
- [ローカルサーバ] 機能のリストにはないオンラインゲームやビデオ会議用のソフトウェアで、使用するポートなどの情報が公開されていない場合。
- セキュリティの制限無しに、1 台のパソコンで全てのサービスをインターネットに公開する場合。

ご注意

- DMZ ホストとして、複数のパソコンを設定することはできません。
- DMZ ホストとして設定したパソコンは、ファイアウォールで保護されていないため、外部から攻撃を受ける恐れがあります。
- ローカルサーバ機能と DMZ ホスト機能を同時に設定しているときは、ローカルサーバの設定が優先されます。

インターネットから LAN 側へのアクセス要求を受け取ると、本商品は [ローカルサーバ] 機能で登録されている宛先を除き、すべて DMZ ホストへその要求を転送します。

LAN側のパソコンをDMZホストに設定する

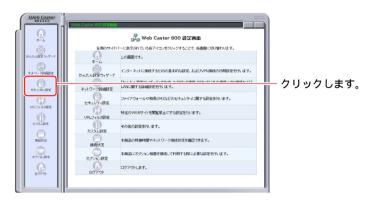
ここでは、LAN側のパソコンをインターネットに公開するためのDMZホストの設定について説明します。

1　サイドバーから[セキュリティ設定]アイコンをクリックします。

2　[DMZホスト]ボタンをクリックします。

3 **［DMZ ホストIP アドレス］欄にチェックを付け、DMZ ホストにするパソコンのIP アドレスを入力します。**

4 **［OK］ボタンをクリックします。**

5 **以上で設定は終了です。**

DMZ ホストの有効/無効の切替

1 **サイドバーから[セキュリティ設定]アイコンをクリックします。**

2 **[DMZ ホスト]ボタンをクリックします。**

3 ［DMZ ホスト IP アドレス］欄からチェックを外します。

4 ［OK］ボタンをクリックします。

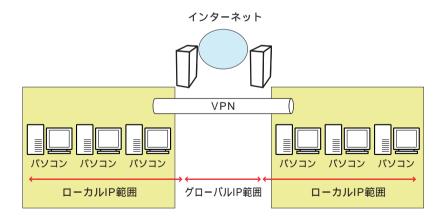
5 以上で設定は終了です。

VPNの設定

VPN（Virtual Private Network）は、データのカプセル化や暗号化などのセキュリティ技術を使って、インターネットを仮想的に、専用線で接続したWANのように利用する技術です。VPNを構築するためには、PPTP（Point to Point Tunneling Protocol）やIPSec（IP Security）などのプロトコルが用いられます。ここでは、PPTPとIPSecによるVPN接続の方法について説明します。
本商品は、PPTPサーバとPPTPクライアントおよびIPSecの機能を搭載しているため、パソコンにVPN用のソフトウェアを導入する必要もなく、強固なセキュリティ機能をもつVPNを構築することができます。
なお、接続可能なVPNトンネルの数は以下の通りです。また、多数の接続を行うとスループットが低下する場合があります。

［PPTPサーバ］
最大32接続(PPPoEのセッション数を含む。推奨10接続程度)

［PPTPクライアント］
1接続のみ

［IPSec］
最大50接続(推奨10接続程度)

VPNを構築するには、かんたん設定ウィザードによる設定をした後、ネットワーク詳細設定によって、詳細な設定が可能です。次ページのかんたん設定ウィザードから設定を進めてください。なお、すでにかんたん設定ウィザードによるVPN接続設定が終わっている場合は、P.6-179の「ネットワーク詳細設定による設定」に進んでください。

ご注意

VPNトンネルにおいて、パケットフィルタリングは適用できません。VPNトンネルを利用した特定のパケットについて制限をかける場合には、LANポート側で設定を行うようお願いいたします。

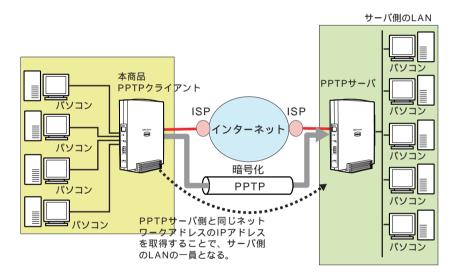
ご注意

本商品で接続確認を行っている相手側装置は本商品のみになります。
他商品との接続はお客様の責任において行ってください。

かんたん設定ウィザードによる設定

ここでは、かんたん設定ウィザードを使いVPNを構築する方法について説明します。
本商品はPPTPサーバ、PPTPクライアント、IPSecに対応しています。ご利用する環境に合わせて設定を進めてください。

PPTPクライアントの設定

本商品をPPTPクライアントとして使用する場合の設定について説明します。

ご注意

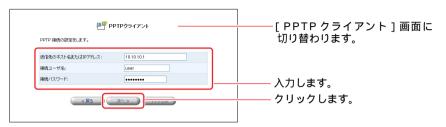
- PPTPクライアント側のネットワークアドレスとPPTPサーバ側のネットワークアドレスが重なっている場合は接続できません。必ず異なるネットワークアドレスにしてください。
- PPTPクライアント側のネットワークからPPTPサーバ側ネットワークへは通常NAPTを使用して接続しています。PPTPサーバ側ネットワークのパソコンからPPTPクライアント側のネットワークのパソコンを直接指定した通信は出来ません。
- 本商品のPPTPクライアント機能は、本商品のPPTPサーバとのみ接続確認を行っています。

1 **サイドバーから[かんたん設定ウィザード]アイコンをクリックします。**

2 **[VPN接続]を選択し、[次へ]ボタンをクリックします。**

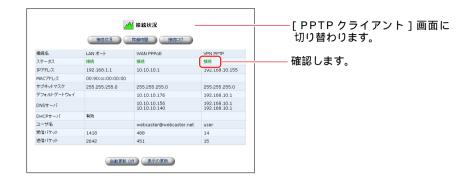
3 **[PPTPクライアント]を選択し、[次へ]ボタンをクリックします**

4 リモートアクセスするサーバの設定に従い、PPTP接続の設定を行います。

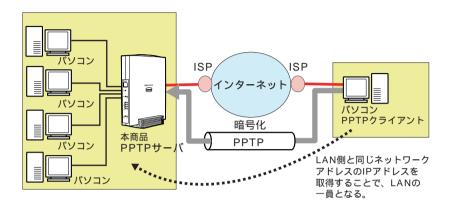
[接続先のホスト名またはIPアドレス]に接続するPPTPサーバのIPアドレスを入力し、[接続ユーザ名]、[接続パスワード]に接続する時のユーザ名とパスワードを入力します。
[次へ]ボタンをクリックします。

5 [接続完了]画面が表示されます。

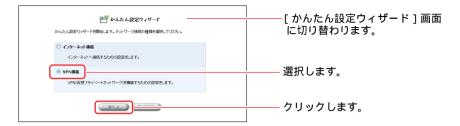
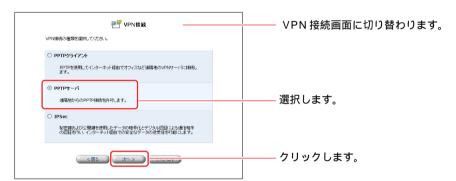
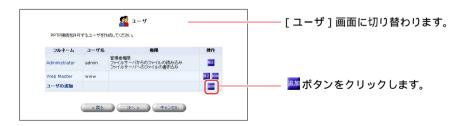
PPTP接続するサーバ名またはIPアドレスを確認し、[完了]ボタンをクリックします。

6 サイドバーから[接続状況]アイコンをクリックします。

7 VPN PPTPが[接続]になっていることを確認します。

8 以上でPPTPクライアントの設定は完了です。

PPTP サーバの設定

本商品を PPTP サーバとして使用する場合の設定について説明します。

1　**サイドバーから[かんたん設定ウィザード]アイコンをクリックします。**

2 [VPN 接続]を選択し、[次へ]ボタンをクリックします。

3 [PPTP サーバ]を選択し、[次へ]ボタンをクリックします。

4 PPTP サーバにアクセスを許可する為のユーザ設定を行います。

5 ［一般設定］欄のフルネーム、ユーザ名、新しいパスワード、新しいパスワードの確認に登録するユーザの設定を入力し、［権限］欄から［PPTP リモートアクセス］にチェックをつけます。

6 ユーザの追加または修正、削除が終わると［ユーザ］画面に戻りますので、［次へ］ボタンをクリックします。

7　PPTPクライアントのリモートアドレスを入力します。

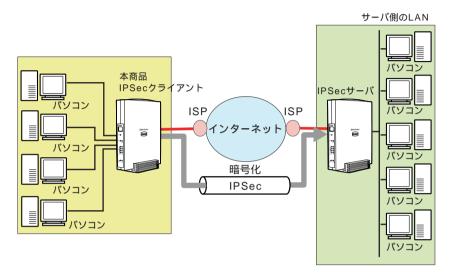
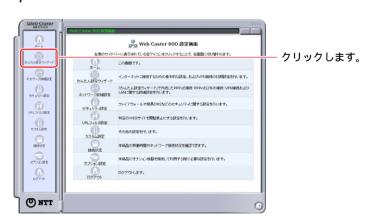
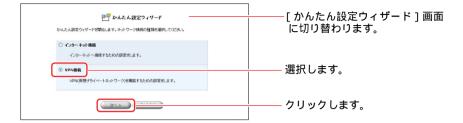
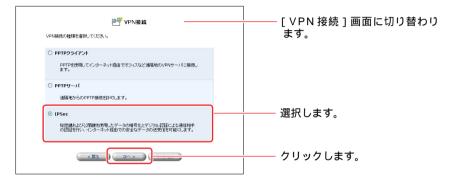
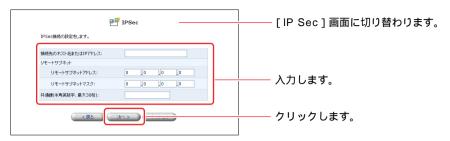
PPTPサーバにリモートアクセスするユーザに割り当てるIPアドレスの範囲（LANポートに設定したIPアドレと同じネットワークのIPアドレス）を入力し、［次へ］ボタンをクリックします。

8　[設定完了]画面が表示されます。

[完了]ボタンをクリックします。

インターネットに接続されている場合、PPTPクライアントの設定が完了すると、自動的にPPTPサーバへ接続を行います。

IPSecの設定

本商品を使いIPSecによるVPN接続を行う場合の設定について説明します。本商品のIPSec機能は、2つのネットワークを常時接続することを想定しています。2つ以上の接続を行う場合は、各ネットワークのネットワークアドレスが重ならないようにして下さい。

1 **サイドバーから[かんたん設定ウィザード]アイコンをクリックします。**

2 ［VPN 接続］を選択し、［次へ］ボタンをクリックします。

3 ［IPSec］を選択し、［次へ］ボタンをクリックします。

4　接続するIPSecの情報を入力し、［次へ］ボタンをクリックします。

［接続先のホスト名またはIP アドレス］

IPSecで接続する相手側のホスト名またはIP アドレスを入力します。

［リモートサブネットアドレス］

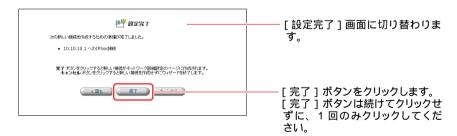
IPsecで接続する相手側のネットワークアドレスを入力します。

［リモートサブネットマスク］

IPSecで接続する相手側のサブネットマスクを入力します。

［共通鍵］

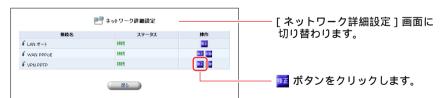
IPSec間で認証を行うときに使う事前共有鍵を入力します。
鍵の値は両方のルータで同じ値を入力します。

5　［設定完了］画面が表示されます。［完了］ボタンをクリックします。

ネットワーク詳細設定による設定

PPTP クライアントやサーバに関する詳細な設定と、IPSec の詳細設定について説明します。
VPN の詳細な設定をするためには、あらかじめ「かんたん設定ウィザード」による設定を終了しておく必要があります。未設定の場合は、P.6-168 に戻って設定してください。

PPTP クライアントの詳細設定

1 **サイドバーから[ネットワーク詳細設定]アイコンをクリックします**

2 **[ネットワーク詳細設定]画面が表示されます。詳細な設定を行う VPN PPTP 接続の[修正]ボタンをクリックします。**

3 ［ネットワーク詳細設定 VPNPPTP］画面が表示されます。接続名、ステータス、ユーザ名等が表示されていますので、確認して［詳細設定］ボタンをクリックします。

4 ［詳細設定 VPNPPTP］画面が表示されます。PPTP サーバ管理者の通知に従って、基本設定、PPP、PPP 認証、PPP 暗号化、IP の設定方法などを設定します。

◎基本設定、PPP、PPP 認証の設定

［接続先のホスト名または IP アドレス］、［接続ユーザ名］、［接続パスワード］には、かんたん設定ウィザードで設定した内容が表示されています。変更する必要がある項目を修正します。

ユーザ認証のためのプロトコルを選択します。［PPP 暗号化］で「暗号化を許可する」場合は、MS-CHAP または MS-CHAP v2 を選択します。

◎ PPP暗号化、IP設定

パケットの暗号化に関する設定を行います。

[PPP暗号化]

- 暗号化を必ず要求する：
  暗号化通信を要求するときにチェックします。サーバが拒否するとPPTP通信は確立されません。
- 暗号化を許可する：
  暗号化にMPPE(Microsoft Point-to-Point Encryption)を使用します。40bitのキーで暗号化するか、128bitのキーを使うかで、MPPE-40 BitかMPPE-128 Bitを選択します。
- MPPE暗号化モード：
  暗号化のモード(Stateless または Stateful)を選択します。Statelessはパケットごとに暗号化キーを変更するので、通信の安全性は高くなります。Statefulは 複数のパケット単位で暗号化キーを変更します。
  暗号化を許可する場合は、[PPP認証]で、MS-CHAPまたは、MS-CHAP v2が選択されていることを確認してください。

[IP設定]

IPアドレスを固定にするか、自動取得にするかを選択します。固定にする場合は、IPアドレスを入力します。

[DNSサーバ]

DNSサーバアドレスを自動取得するのか、固定設定にするのか選択します。固定にする場合は、プライマリとセカンダリDNSサーバのIPアドレスを指定します。

[デバイスメトリック]

メトリックの値を入力します。

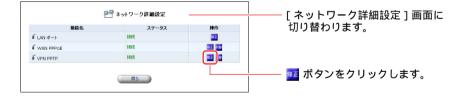
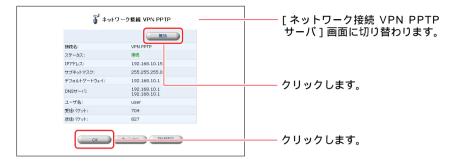
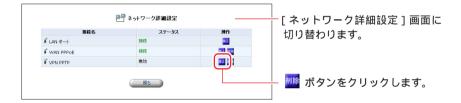
ルーティング・テーブル上に利用可能なルートが複数存在する場合には、このメトリックの小さなルート（インターフェイス）を優先的に使用するようになっています。

5 [OK]ボタンをクリックすると設定が有効になり、[ネットワーク接続 VPN PPTP]画面に戻ります。

PPTPクライアントの削除

ここでは、既に登録してあるPPTPクライアント接続を削除する場合について説明します。

1　サイドバーから[ネットワーク詳細設定]アイコンをクリックします

2　[接続名]欄から削除するVPN PPTP接続の[修正]ボタンをクリックします。

3 **回線が接続されてる場合は、[無効]ボタンをクリックし、回線をいったん切断します。[OK]ボタンをクリックします。**

4 **[接続名]欄から削除するVPN PPTP接続の[削除]ボタンをクリックします。[削除]ボタンは続けてクリックせずに、1回のみクリックしてください。**

5 **[戻る]ボタンをクリックします。**

6 **以上で設定は終了です。**

PPTPサーバの詳細設定

1　サイドバーから[ネットワーク詳細設定]アイコンをクリックします。

クリックします。

2　[ネットワーク詳細設定]画面が表示されます。詳細な設定を行うVPN PPTPサーバ接続の[修正]ボタンをクリックします。

※ PPTPサーバを削除する場合は、[削除]ボタンをクリックするか、あるいは[修正]ボタンをクリックして、[PPTPサーバ]画面の[有効]欄からチェックを外します。

3 **［PPTP サーバ］画面が表示されます。**
［詳細設定］ボタンをクリックします。
なお、ここでユーザの編集、PPTP クライアントの接続設定も可能です。

4 **［PPTP サーバ］画面が表示されます。PPTP サーバの詳細な設定を行います。**

［ステータス］

PPTP サーバの接続状況を表示します。

［有効］

PPTP サーバを有効にするときにチェックします。このチェックをはずすと、PPTP サーバとして動作しなくなり、接続状況にも反映されなくなり、また詳細設定の画面からも削除されます。

［ユーザ］

クリックすると、ユーザの設定を行うことができます。

[自動切断までの時間]
PPTPによる通信が中断したときに、接続を切断するまでの時間を分単位で入力します。

[許可する認証アルゴリズム]
ユーザセキュリティで[認証が必要]にチェックした場合、認証のアルゴリズムをPAP、CHAP、MS-CHAP-v1、MS-CHAP-v2から選択します。次の[暗号化が必要]にチェックをした場合は、MS-CHAP-v1かMS-CHAP-v2をチェックして下さい。

- [認証が必要]：
  PPTPクライアントが接続する際に、ユーザ認証を必要とするときにチェックします。接続テストなど特別な場合を除いて必ずチェックを入れてください。

[許可する暗号化アルゴリズム]
ユーザセキュリティで[暗号化が必要]にチェックした場合、暗号化アルゴリズムをMPPE-40とMPPE-128から選択します。

- [暗号化が必要]：
  PPTPクライアントが接続するときに、暗号化通信を要求する場合にチェックします。

[MPPE暗号化モード]
暗号化のモード(Stateless または Stateful)を選択します。

- Stateless：
  パケットごとに暗号化キーを変更するので、通信の安全性は高くなります。
- Stateful：
  複数のパケット単位で暗号化キーを変更します。

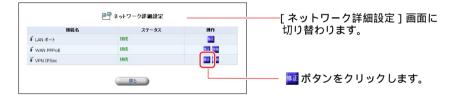
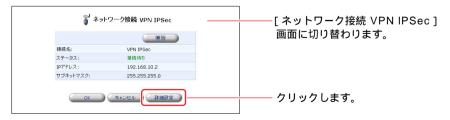
5 [かんたん設定ウィザード]で設定した、リモートアドレス範囲、クライアントとして動作する場合のPPTPクライアントの設定が表示されます。クリックし修正することが可能です。

確認します。

6 [OK]ボタンをクリックすると、設定が有効になりネットワーク詳細設定画面に戻ります。[基本設定]ボタンをクリックすると、PPTPサーバの最初の画面に戻ります。

IPSecの詳細設定

1 **サイドバーから[ネットワーク詳細設定]アイコンをクリックします**

2 **[ネットワーク詳細設定]画面が表示されます。詳細な設定を行うVPN IPSec接続の[修正]ボタンをクリックします。**

3 **[ネットワーク接続 VPN IPSec]画面が表示されます。[詳細設定]ボタンをクリックします。**

4 「詳細設定 VPN IPSec」画面が表示されます。

［詳細設定 VPN IPSec］画面に切り替わります。

ここで次の項目を設定します。

基本設定

[接続先のホスト名またはIP アドレス]

かんたん設定ウィザードで設定した接続先が表示されています。必要であれば修正します。

[ローカルサブネット]

本商品のLAN側のサブネットアドレス、サブネットマスクを設定します。

[リモートサブネット]

接続先のサブネットアドレスとサブネットマスクを入力します。

[データ圧縮]

データ圧縮をするときにチェックします。

[鍵交換方式]

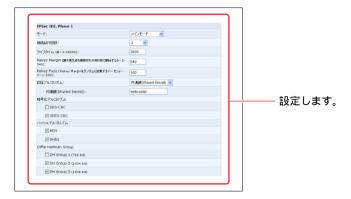
暗号化アルゴリズムや鍵交換のためのSAの合意をとる方式を選択します。

- 自動：
  IKE（Internet Key Exchange）を使って、SAの合意を通信時に自動的に行う場合に選択します。通常は、自動に設定しておきます。
- 手動：
  SAの合意をあらかじめ手動で設定しておく場合に選択します。画面が手動用に切り替わります。

5　鍵交換方式を自動に設定します。

鍵交換方式を［自動］に設定した場合、次の 2 つのフェーズの設定を行います。まず、IPSec IKE, Phase 1 の設定をします。

IPSec IKE, Phase 1

［モード］

モードを選択します。

- メインモード
- アグレッシブモード

［接続試行回数］

ネゴシエーションの試行回数を設定します。

［ライフタイム］

鍵の有効期限を秒単位で設定します。

［Rekey Margin］

Rekey（鍵の再生成）を期限切れの何秒前に開始するかを設定します。

［Rekey Fuzz］

Rekey Margin に対する最大の増分値をパーセンテージで設定します。例えば、Rekey Margin を 540 秒、Rekey Fuzz を 100 %に設定した場合は、Rekey Margin の最大の増分値は 540 秒（540 秒の 100 %）となり、実際に Rekey Margin が取り得る値は、540 ～ 1080 秒の間となります。

［認証アルゴリズム］

認証の方式を選択します。

- 共通鍵：
  共通鍵方式を選択する場合は、事前共有キーの文字列を入力します。
  （かんたん設定ウィザードで入力した鍵が表示されます。）
- 公開鍵：
  公開鍵方式を使用する場合に、キーの文字列を入力します。

[暗号化アルゴリズム]

使用する暗号化アルゴリズムを選択します。

[ハッシュアルゴリズム]

使用するハッシュのアルゴリズムを選択します。

[Diffie-Hellman-Group]

対応するグループを選択します。

ワンポイント

メインモードは、双方が固定のIPの環境での接続に向いており、双方のIPが固定されているため、よりセキュリティの高い接続可能です。アグレッシブモードはIPアドレスが動的に変わる環境での利用に向いています。ただし、本商品はIPアドレスを用いた認証を行うため、相手側接続機器の仕様に依存します。

6　次にIPSec IKE, Phase 2の設定をします。

IPSec IKE, Phase 2

[ライフタイム]

鍵の有効期限を秒単位で設定します。

[PFS有効]

Secrecy(PFS)を使用する場合にチェックします。

[Diffie-Hellman-Group]

対応するグループを選択します。

[暗号化アルゴリズム]

使用する暗号化アルゴリズムを選択します。

[認証アルゴリズム]

使用する暗号化アルゴリズムを選択します。

[ハッシュアルゴリズム]

認証ヘッダの設定をします。ハッシュアルゴリズムを選択します。

[デバイスメトリック]

メトリックの値を入力します。

ルーティング・テーブル上に利用可能なルートが複数存在する場合には、このメトリックの小さなルート（インターフェイス）を優先的に使用するようになっています。

7 **詳細設定 VPN IPSec画面の設定内容を確認し、[OK]ボタンをクリックして、設定を有効にします。**

8 **IPSecを利用しVPNを構築する場合は、IPフラグメントパケットを透過させる必要がありますので、セキュリティ設定画面で、[IPフラグメントパケットを遮断する]のチェックをはずしてください。**

鍵交換方式を手動に設定する場合

鍵交換方式で手動を選択したときは、接続先の設定にあわせて暗号化アルゴリズム、認証アルゴリズムを設定する必要があります。

暗号化アルゴリズム、認証アルゴリズムのキーは、16 進数 8 桁ずつに区切って入力してください。

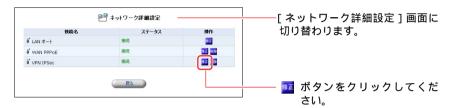
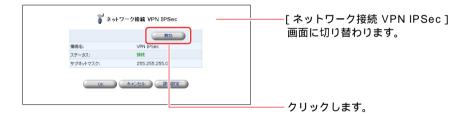
VPNの接続、切断

サーバ側、クライアント側でインターネットに接続すると、自動的にLAN同士が接続されます。

1 **IPSecによる通信を切断したい場合は、［ネットワーク詳細設定］画面で、［VPN IPSec］の［修正］ボタンをクリックします。**

［ネットワーク詳細設定］画面に切り替わります。

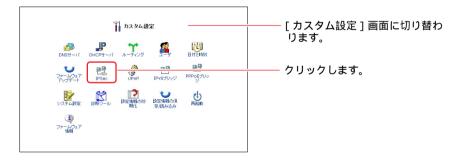
修正 ボタンをクリックしてください。

2 **［ネットワーク接続VPN IPSec］画面になりますので、［無効］ボタンをクリックします。**

［ネットワーク接続 VPN IPSec］画面に切り替わります。

クリックします。

鍵の再生成

IPSec 接続に関してその他次の設定が可能です。

1　サイドバーから［カスタム設定］アイコンを選択します。

2　［IPSec］アイコンをクリックします。

3　［IPSec］画面が表示されます。［詳細設定ボタン］をクリックします。

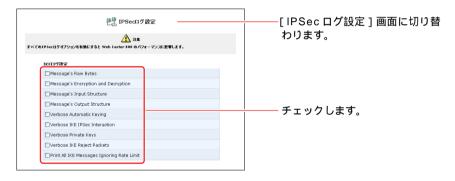
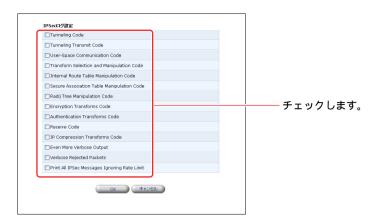
4 **［IPSec設定］画面が表示されます。［鍵の再生成］ボタンをクリックし、再生成を行います。**

5 **表示の更新ボタンをクリックすると、再生成されたキーが表示されます。［戻る］ボタンをクリックすると［IPSec］画面に戻ります。**

IPSec ログの設定

IPSec 通信のログに関する設定を変更することができます。

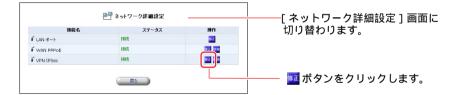
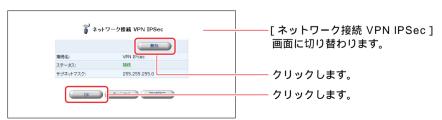
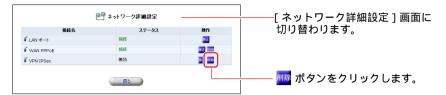
1　カスタム設定で[IPSec]アイコンをクリックし、IPSec 画面で[ログ設定]ボタンをクリックします。

2　[IPSec ログ設定]画面が表示されます。記録したい内容にチェックをつけます。

3 **[OK]ボタンをクリックすると設定が有効になり、[IPSec]画面に戻ります。**

IPSecの削除

ここでは、既に登録してあるIPSec接続を削除する場合について説明します。

1　サイドバーから[ネットワーク詳細設定]アイコンをクリックします

2　[接続名]欄から削除するVPN IPSec接続の[修正]ボタンをクリックします。

3　回線が接続されてる場合は、[無効]ボタンをクリックし、回線をいったん切断します[OK]ボタンをクリックします。

4 **[接続名]欄から削除するVPN IPSec接続の[削除]ボタンをクリックします。**
[削除]ボタンは続けてクリックせずに、1回のみクリックしてください。

5 **[戻る]ボタンをクリックします。**

6 **以上で設定は終了です。**

オプション設定

ここでは、本商品のファイルサーバ、FTP サーバ、Web サーバ、追加機能パッケージ、USB カメラサーバについて説明します。

ファイルサーバの設定

本商品に USB ストレージデバイスを接続するとファイルサーバとして機能します。
ここでは USB ストレージデバイスを利用するための概要をまとめます。

お知らせ

追加機能パッケージ「PHP 対応 Web サーバ」をインストールすることにより、PHP 対応 Web サーバをご利用になることができます。PHP 対応 Web サーバについてはP.6-284 の「PHP 対応 Web サーバの機能」をご覧ください。

本商品に USB ストレージデバイスを接続します。

↓

USB ストレージデバイスのパーティションを作成し、フォーマットします。

↓

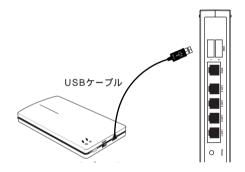
ワークグループの設定をします。

↓

ユーザーアカウントの作成をします。

Web Caster 800へのUSBストレージデバイスの取り付け

1 **Web Caster 800電源アダプタを取り外し、Web Caster 800の電源を完全に切ります。USBストレージデバイスの電源が切れていることを確認します。**

2 **USBストレージデバイスを本商品に接続します。USBストレージデバイスに付属のUSBケーブルを使用して、本商品のUSBポートにハードディスクを接続します。**

3 **USBストレージデバイスの電源を入れます。**

ご注意

本商品はUSBストレージデバイスのバスパワー動作はサポートしておりませんので、USBストレージデバイスは付属のACアダプタを使用するなどしてセルフパワーで動作させてください。

4 **本商品の電源を入れてください。**

次にWeb Caster 800からUSBストレージデバイスのパーティションの設定を行います。

パーティションの種類

パーティションの種類には「プライマリパーティション」,「拡張パーティション」,「論理パーティション」があります。
「プライマリパーティション」は、１つのハードディスクに最大４個まで作成可能です。「拡張パーティション」はそれ自体ではドライブとして認識されません。ただし「拡張パーティション」内に「論理ドライブ」を複数作成することができます。（作成できる論理ドライブ数は最大11個まででです。）

ご注意

・本商品のフォーマット方法でEXT2を選択する場合は、パーティションサイズを137438MB（137GB）以下でご使用ください。137GB以上のパーティションをご利用の場合は、FAT32形式でフォーマットをご使用ください。
・ドライブ文字はUSB ストレージデバイスをマウント時（接続したまま本商品を再起動した場合も含む）に自動的に基本領域、拡張領域の順に割り振られます。そのため、基本領域で割り当てられたドライブ番号（A,B など）を先に削除した場合や、先頭または途中にある未領域にドライブを割り当てた場合、ドライブ文字が入れ替わることがあります。領域を削除する場合は最後の領域から削除するようにして下さい。
・12個以上の論理パーティションがあるUSBストレージデバイスを接続した場合、12個目以降の論理パーティションをファイルサーバ機能で使用することはできません。

USB ストレージデバイスのパーティション作成

USB ストレージデバイスを接続したら、パーティションの作成とフォーマットを行う必要があります。ここではパーティションの作成手順を説明します。

1　**サイドバーから［オプション設定］アイコンをクリックします。**

2　**［オプション設定］画面が表示されます。［ファイルサーバ］アイコンをクリックします。**

3 ［ファイルサーバ］設定画面が表示されます。［詳細］に接続されているハードディスク名が表示されます。パーティションを設定するハードディスク名をクリックします。

ご注意

［詳細］に表示されるハードディスク名はご使用になられているハードディスクによって変わります。マニュアルと同じ表記になるとは限りませんのでご注意ください。

4 ［ディスク情報］設定画面が表示されます。［パーティション］に接続されているハードディスクのパーティション情報が表示されます。［パーティション］には以下の情報が表示されます。

[共有名]

ネットワーク上で表示される共有ドライブ名です。共有名はWeb Caster 800ホスト名とパーティション作成時に割り当てられたドライブ文字から自動的に作成されます。

[タイプ]

パーティションのフォーマット形式です。Windows FAT32、FAT16またはLinuxのいずれかが表示されます。

[ステータス]

パーティションの現在の状態が表示されます。フォーマット中はフォーマット状況が表示されます。［使用可］と表示されているパーティションがアクセス可能です。

[容量]

パーティションに割り当てられている容量です。

[空き容量]

パーティションの空き容量です。［容量］から［空き容量］を引いた分がパーティションの使用されている容量です。

[操作]

パーティションの操作を行います。

! ご注意

［共有名］に［未使用の領域］と表示されている部分はパーティションが作成されていないハードディスク領域です。

5　［未使用の領域］の［操作］から［追加］ボタンをクリックします。

6　［パーティションタイプ］設定画面が表示されます。作成するパーティションタイプを選択して［次へ］ボタンをクリックします。

［プライマリパーティション］を選択した場合は、P.6-208［プライマリパーティションの作成］に進みます。［拡張パーティション］を選択した場合はP.6-211［拡張パーティションと論理パーティションの作成］に進みます。

プライマリパーティションの作成

1 ［パーティションタイプ］設定画面で［プライマリパーティション］を選択して［次へ］ボタンをクリックします。

2 ［パーティションサイズ］設定画面が表示されます。［パーティションサイズ］に作成したいパーティションのサイズを入力して［次へ］ボタンをクリックします。パーティションサイズは最小サイズ〜最大サイズの範囲で設定できます。

ご注意

本商品は1GB=1024MBで計算します。

3 ［パーティションのフォーマット］設定画面が表示されます。［フォーマットを行う］を選択して［次へ］ボタンをクリックします。

4 ［ファイルシステムの選択］設定画面が表示されます。［ファイルシステム］からフォーマットに使用するファイルシステムを選択して［次へ］ボタンをクリックします。

ご注意

本商品のフォーマット方法でEXT2を選択する場合は、パーティションサイズを137438MB（137GB）以下でご使用ください。137GB以上のパーティションをご利用の場合は、FAT32形式でフォーマットをご使用ください。

5 ［パーティションの作成］設定画面が表示されます。［完了］ボタンをクリックします。

6 パーティションが作成され［ディスク情報］設定画面に戻ります。作成したパーティションの［ステータス］が［フォーマット中］と表示されているときはパーティションのフォーマットを行っていますので、ディスクにアクセスできません。［ステータス］が［使用可］になるまでお待ちください。

! ご注意

［ステータス］がフォーマットのまま変わらないときは、しばらく待ってから［表示の更新］ボタンを押してください。

7 ［未使用の領域］が残っている場合は、同様の手順でさらに追加のパーティションを作成する事ができます。

拡張パーティションと論理パーティションの作成

1　［パーティションタイプ］設定画面で［拡張パーティション］を選択して［次へ］ボタンをクリックします。

2　［パーティションサイズ］設定画面が表示されます。［パーティションサイズ］に作成したいパーティションのサイズを入力して［次へ］ボタンをクリックします。パーティションサイズは最小サイズ〜最大サイズの範囲で設定できます。

ご注意

本商品は1GB=1024MBで計算します。

3 ［パーティションの作成］設定画面が表示されます。［完了］ボタンをクリックします。

4 パーティションが作成され［ディスク情報］設定画面に戻ります。作成された［拡張パーティション］の［未使用の領域］の［操作］から［追加］ボタンをクリックします。

5 ［パーティションタイプ］設定画面が表示されます。［次へ］ボタンをクリックします。

6 ［パーティションサイズ］設定画面が表示されます。［パーティションサイズ］に作成したいパーティションのサイズを入力して［次へ］ボタンをクリックします。パーティションサイズは最小サイズ～最大サイズの範囲で設定できます。

! ご注意

本商品は1GB=1024MBで計算します。

7 ［パーティションのフォーマット］設定画面が表示されます。［フォーマットを行う］を選択して［次へ］ボタンをクリックします。

8 ［ファイルシステムの選択］設定画面が表示されます。［ファイルシステム］からフォーマットに使用するファイルシステムを選択して［次へ］ボタンをクリックします。

ご注意

本商品のフォーマット方法でEXT2を選択する場合は、パーティションサイズを137438MB（137GB）以下でご使用ください。137GB以上のパーティションをご利用の場合は、FAT32形式でフォーマットをご使用ください。

9 ［パーティションの作成］設定画面が表示されます。［完了］ボタンをクリックします。

10 **パーティションが作成され［ディスク情報］設定画面に戻ります。作成したパーティションの［ステータス］が［フォーマット中］と表示されているときはパーティションのフォーマットを行っていますので、ディスクにアクセスできません。［ステータス］が［使用可］になるまでお待ちください。**

ご注意

［ステータス］がフォーマットのまま変わらないときは、しばらく待ってから［表示の更新］ボタンを押してください。

11 **［拡張パーティション］の［未使用の領域］が残っている場合は、同様の手順でさらに追加の論理パーティションを作成する事ができます。**

フォーマット済みのUSBストレージデバイスを接続する場合

本製品にフォーマット済みのハードディスクを接続する場合は以下の点にご注意ください。

本製品がサポートしているハードディスクのフォーマットはFAT16,FAT32,EXT2のみです。それ以外のフォーマットは使用できませんのでコンピュータに接続してフォーマットしなおすか、Web Caster 800上でフォーマットしてください。

USBストレージデバイスのフォーマット

ここではNTFSでフォーマット済みのUSBストレージデバイスをWeb Caster 800に接続してフォーマットするときの手順について説明します。

1 **P.6-202の手順でUSBストレージデバイスをWeb Caster 800に接続します。**

2 **サイドバーから［オプション設定］アイコンをクリックします。**

3 **［オプション設定］画面が表示されます。［ファイルサーバ］アイコンをクリックします。**

4　［ファイルサーバ］設定画面が表示されます。［詳細］に接続されているハードディスク名が表示されます。パーティションを設定するハードディスク名をクリックします。

ご注意

［詳細］に表示されるハードディスク名はご使用になられているハードディスクによって変わります。マニュアルと同じ表記になるとは限りませんのでご注意ください。

5　［ディスク情報］設定画面が表示されます。［パーティション］に接続されているハードディスクのパーティション情報が表示されます。NTFS でフォーマットされているパーティションは「共有名」が「未サポート」と表示されます。

6 「未サポート」と表示されているパーティションの「操作」から「フォーマット」アイコンをクリックします。

7 ［ファイルシステムの選択］設定画面が表示されます。［ファイルシステム］からフォーマットに使用するファイルシステムを選択して［次へ］ボタンをクリックします。

ご注意

本商品のフォーマット方法で EXT2 を選択する場合は、パーティションサイズを 137438MB（137GB）以下でご使用ください。137GB 以上のパーティションをご利用の場合は、FAT32 形式でフォーマットをご使用ください。

8 「注意」画面が表示されます。フォーマットを実行するとパーティション内のデータはすべて消去されます。フォーマットを実行する場合は［OK］をクリックします。

9 パーティションのフォーマットが開始され、［ディスク情報］設定画面に戻ります。パーティションの［ステータス］が［フォーマット中］と表示されているときはパーティションのフォーマットを行っていますので、ディスクにアクセスできません。［ステータス］が［使用可］になるまでお待ちください。

! ご注意

［ステータス］がフォーマットのまま変わらないときは、しばらく待ってから［表示の更新］ボタンを押してください。

10 パーティションのステータスが「使用可」と表示されればフォーマットは完了です。パーティションはファイルサーバやWebサーバとして使用できるようになります。

作成済みのパーティションの削除

ここではUSBストレージデバイスにあるパーティションの削除手順を説明します。

1　サイドバーから［オプション設定］アイコンをクリックします。

2　［オプション設定］画面が表示されます。［ファイルサーバ］アイコンをクリックします。

3　［ファイルサーバ］設定画面が表示されます。［詳細］に接続されているハードディスク名が表示されます。パーティションを設定するハードディスク名をクリックします。

ご注意

［詳細］に表示されるハードディスク名はご使用になられているハードディスクによって変わります。マニュアルと同じ表記になるとは限りませんのでご注意ください。

4　［ディスク情報］設定画面が表示されます。削除したいパーティションの［操作］から［削除］アイコンをクリックします。

5　［注意］画面が表示されます。

この時にパーティションにアクセスしているユーザがいるときは下記のメッセージが表示されます。このメッセージが表示されたときは、ユーザのアクセスが終了するのを待ってからパーティションの削除をしてください。

6　パーティションの削除を続ける場合は［OK］ボタンをクリックします。

! ご注意

パーティションの削除を行うとパーティション内のデータはすべて失われます。パーティションの削除をするときは大事なデータが入っていないことを確認してください。

7 ［ディスク情報］設定画面に戻ります。パーティションが削除されて、未使用の領域が増えている事を確認します。

ハードディスクの取り外し

ここではUSBストレージデバイスをWeb Caster 800から取り外すときの手順について説明します。Web Caster 800からUSBストレージデバイスを取り外すときは必ずアンマウントをしてから取り外します。

1 サイドバーから［オプション設定］アイコンをクリックします。

2 ［オプション設定］画面が表示されます。［ファイルサーバ］アイコンをクリックします。

3 ［ファイルサーバ］設定画面が表示されます。［詳細］に接続されているハードディスク名が表示されます。パーティションを設定するハードディスク名をクリックします。

ご注意

[詳細]に表示されるハードディスク名はご使用になられているハードディスクによって変わります。マニュアルと同じ表記になるとは限りませんのでご注意ください。

4　[ディスク情報]設定画面が表示されます。[アンマウント]ボタンをクリックします。

5　ディスク情報の［ステータス］が［マウントされていません］になっていることを確認します。

ご注意

［アンマウント］ボタンをクリックしたときに［入力エラー］画面が表示されるときは、USBストレージデバイスにユーザがアクセスしています。ユーザのアクセスを終了させてからアンマウントをしてください。ユーザのアクセスがないにもかかわらず［入力エラー］が表示されるときはセッションが残っている場合があります。この場合は10分経過するとセッションが切れますので、10分ほどお待ちになってからアンマウントしてください。

6　USBストレージデバイスの電源を落とし、USBケーブルをWeb Caster 800から取り外します。

アクセス設定

本商品にUSBストレージデバイスを接続した時点でファイルサーバとして動作しますが、作成したパーティションにアクセスする為にはワークグループの設定とユーザアカウントの作成が必要になります。

ここではワークグループ名の設定とユーザアカウントの作成について説明します。

ワークグループ名の設定

コンピュータがファイルサーバにアクセスする為には、コンピュータとWeb Caster 800のワークグループ名が同じである必要があります。

1 サイドバーから［オプション設定］アイコンをクリックします。

2 ［オプション設定］画面が表示されます。［ファイルサーバ］アイコンをクリックします。

3 ［ファイルサーバ］設定画面が表示されます。［NetBIOS ワークグループ名］にコンピュータに設定してあるワークグループ名を入力します。［OK］ボタンをクリックします

ご注意

ファイルサーバにアクセスするコンピュータのワークグループはすべて同じにしておいてください。ワークグループが違う場合にはコンピュータのマイネットワークにファイルサーバが表示されません。

4 ［オプション設定］画面に戻ります。

つづいてユーザアカウントの作成を行います。

ユーザアカウントの作成

1　**サイドバーから［カスタム設定］アイコンをクリックします。**

2　**［カスタム設定］画面が表示されます。［ユーザ］アイコンをクリックします。**

3 ［ユーザ］設定画面が表示されます。［ユーザの追加］の［追加］ボタンをクリックします。

4 ［ユーザ］設定画面が表示されます。P.6-301「ログインユーザ名・ログインパスワード設定」の［ユーザの新規作成］の手順で、フルネーム、ユーザ名、パスワードを設定します。

! ご注意

ユーザの使用するOSがWindows®の場合はユーザ名とパスワードはユーザのWindows®へのログインネームとログインパスワードと同じに設定します。

5 ［権限］からユーザのファイルサーバへのアクセス権限を選択します。

[ファイルサーバからのファイルの読み込み]
この権限にチェックの入っているユーザはファイルサーバのデータを読み出す事が出来ます。

[ファイルサーバへのファイルの書き込み]
この権限にチェックの入っているユーザはファイルサーバにデータを書き込む事が出来ます。またこの権限ではファイルサーバのデータの消去をする事も出来ます。

ご注意

書き込みの権限があるユーザには必ず読み込みの権限も付けてください。読み込みの権限のみか読み込みと書き込みの両方の権限のいずれかに設定してください。

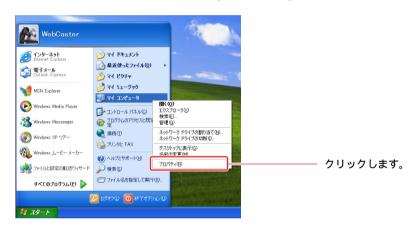
6 ［OK］ボタンをクリックします。アカウントが作成され［ユーザ］設定画面に戻ります。

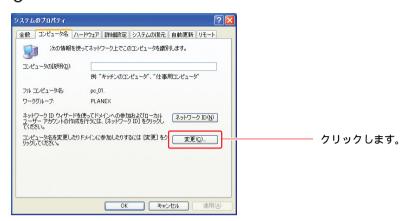
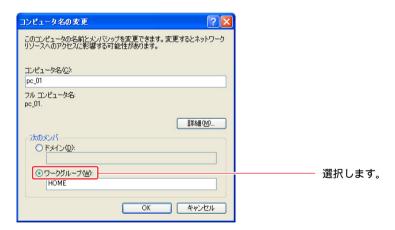
ファイルサーバへのアクセス

ここでは各OS毎のファイルサーバへのアクセス手順について説明します。Windows® ではWeb Caster 800の［NetBIOSワークグループ名］とWindows® のワークグループを同じに設定します。

ワークグループの設定

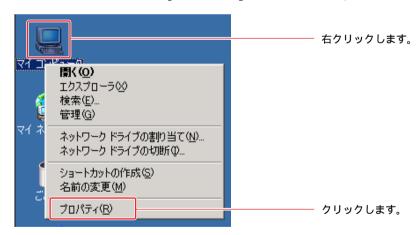
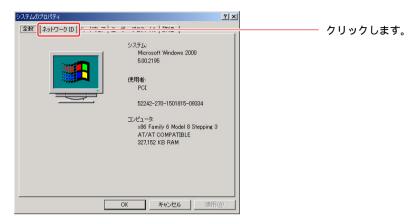
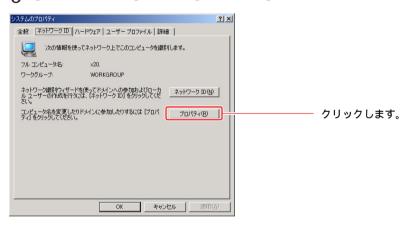
Windows® XP

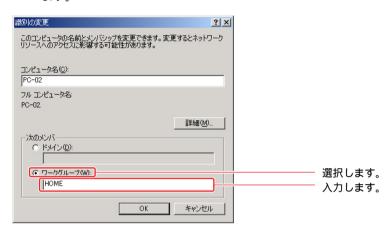
1 ［スタート］メニューから［マイ コンピュータ］アイコンを右クリックします。表示されるメニューから［プロパティ］をクリックします。

2 ［システムのプロパティ］ウィンドウが表示されます。［コンピュータ名］タブをクリックします。

3 ［コンピュータ名］タブから［変更］ボタンをクリックします。

4 ［コンピュータ名の変更］ウィンドウが表示されます。［次のメンバ］から［ワークグループ］を選択します。［ワークグループ］にP.6-228で入力したWeb Caster 800の［NetBIOSワークグループ名］と同じ値を入力します。

5　［OK］ボタンをクリックします。［コンピュータ名の変更］ウィンドウが表示されます。［OK］ボタンをクリックします。

6　［システムのプロパティ］ウィンドウに戻ります。［OK］ボタンをクリックします。再度、［コンピュータ名の変更］ウィンドウが表示されます。［OK］ボタンをクリックしてコンピュータを再起動します。

Windows® 2000

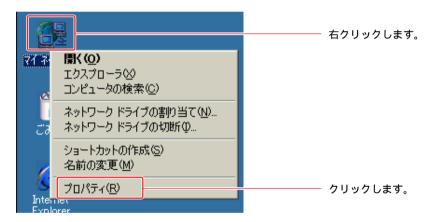
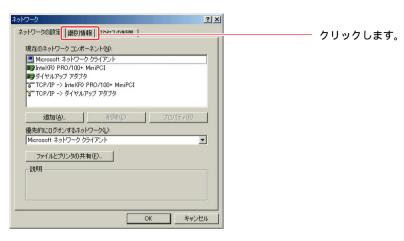
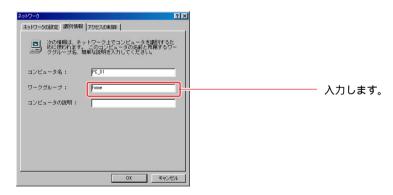
1　デスクトップ上の［マイ コンピュータ］アイコンを右クリックします。表示されるメニューから［プロパティ］をクリックします。

2　［システムのプロパティ］ウィンドウが表示されます。［ネットワークID］タブをクリックします。

3　［ネットワークID］タブから［プロパティ］ボタンをクリックします。

4 ［識別の変更］ウィンドウが表示されます。［次のメンバ］から［ワークグループ］を選択します。［ワークグループ］にP.6-228で入力したWeb Caster 800の［NetBIOSワークグループ名］と同じ値を入力します。

P.6-228

5 ［OK］ボタンをクリックします。［ネットワークID］ウィンドウが表示されるので［OK］ボタンをクリックします。

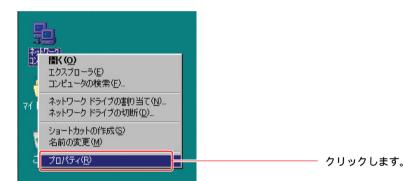
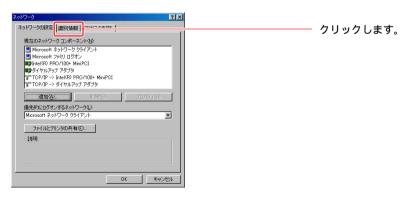
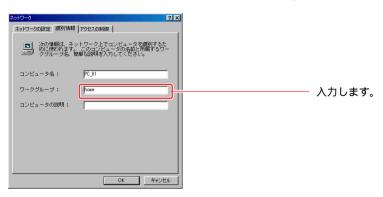
6 再度、［ネットワークID］ウィンドウが表示されるので［OK］ボタンをクリックします。［OK］ボタンをクリックします。

7　［システムのプロパティ］ウィンドウに戻ります。［OK］ボタンをクリックします。［システム設定の変更］ウィンドウが表示されます。［OK］ボタンをクリックしてコンピュータを再起動します。

Windows®Me

1　デスクトップ上の［マイ ネットワーク］アイコンを右クリックします。表示されるメニューから［プロパティ］をクリックします。

2 ［ネットワーク］ウィンドウが表示されます。［識別情報］タブをクリックします。

3 ［識別情報］タブの［ワークグループ］にP.6-228で入力したWeb Caster 800の［NetBIOSワークグループ名］と同じ値を入力します。

4 ［OK］ボタンをクリックします。［システムの設定変更］ウィンドウが表示されます。［はい］ボタンをクリックしてコンピュータを再起動します。

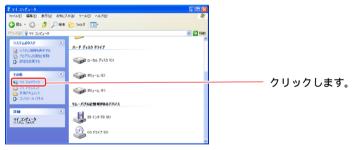
Windows® 98/98Second Edition

1 デスクトップ上の［マイ ネットワーク］アイコンを右クリックします。表示されるメニューから［プロパティ］をクリックします。

2 ［ネットワーク］ウィンドウが表示されます。［識別情報］タブをクリックします。

3 **［識別情報］タブの［ワークグループ］にP.6-228で入力したWeb Caster 800の［NetBIOSワークグループ名］と同じ値を入力します。**

4 **［OK］ボタンをクリックします。［システムの設定変更］ウィンドウが表示されます。［はい］ボタンをクリックしてコンピュータを再起動します。**

ファイルサーバへのアクセス

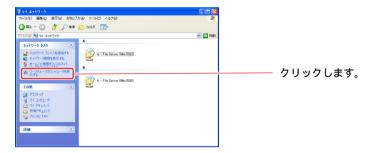
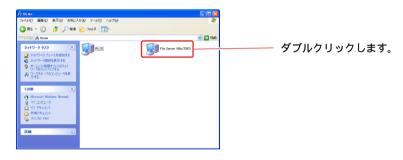
Windows® XP

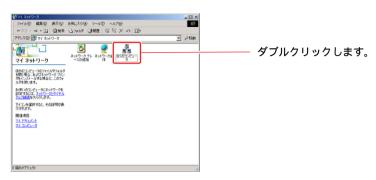
1 ［スタート］メニューから［マイ コンピュータ］アイコンをダブルクリックします。

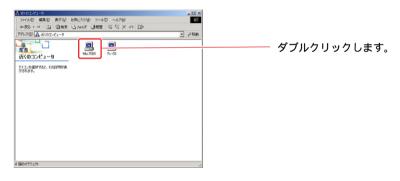
2 ［マイ コンピュータ］ウィンドウが表示されます。ウィンドウ左側から［マイ ネットワーク］アイコンをクリックします。

3 ［マイ ネットワーク］ウィンドウが表示され、ファイルサーバの各パーティションのアイコンが表示されます。アクセスしたいパーティションのアイコンをダブルクリックします。

ご注意

ユーザ名とパスワードを求められる場合はWeb Caster 800にユーザが登録されていません。P.6-229「ユーザアカウントの作成」の手順でWeb Caster 800に登録してあるユーザ名とパスワードを入力してください。

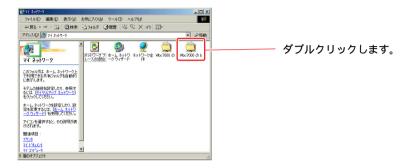
4 ［マイ ネットワーク］ウィンドウにファイルサーバの各パーティションのアイコンが表示されない場合は、［マイ ネットワーク］ウィンドウ左側の［ワークグループのコンピュータを表示する］をクリックします。

5 同じワークグループのコンピュータの一覧が表示されます。［File Server］アイコンがWeb Caster 800のファイルサーバです。［File Server］アイコンをダブルクリックすると各パーティションのアイコンが表示されますのでアクセスするパーティションのアイコンをダブルクリックします。

Windows® 2000

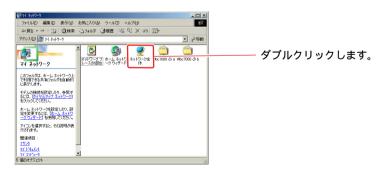
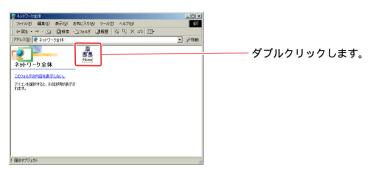
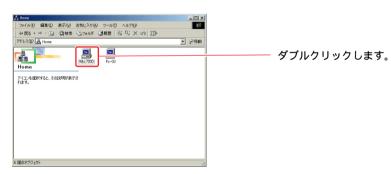
1 デスクトップ上の［マイ ネットワーク］アイコンをダブルクリックします。
［マイ ネットワーク］ウィンドウが表示されます。［近くのコンピュータ］アイコンをダブルクリックします。

2 ［近くのコンピュータ］ウィンドウが表示されます。コンピュータの一覧が表示されます。P.6-309［Web Caster 800のホスト名］に設定した名前のアイコンがWeb Caster 800のファイルサーバです。アイコンをダブルクリックすると各パーティションのアイコンが表示されますのでアクセスするパーティションのアイコンをダブルクリックします。

! ご注意

ユーザ名とパスワードを求められる場合はWeb Caster 800にユーザが登録されていません。P.6-229「ユーザアカウントの作成」の手順でWeb Caster 800に登録してあるユーザ名とパスワードを入力してください。

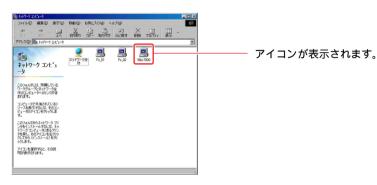
Windows® Me

1 **デスクトップ上の［マイ ネットワーク］アイコンをダブルクリックします。**
［マイ ネットワーク］ウィンドウが表示され、ファイルサーバの各パーティションのアイコンが表示されます。アクセスしたいパーティションのアイコンをダブルクリックします。

ご注意

ユーザ名とパスワードを求められる場合はWeb Caster 800にユーザが登録されていません。P.6-229「ユーザアカウントの作成」の手順でWeb Caster 800に登録してあるユーザ名とパスワードを入力してください。

2 **［マイ ネットワーク］ウィンドウにファイルサーバの各パーティションのアイコンが表示されない場合は、［ネットワーク全体］アイコンをダブルクリックします。**

3 ［ネットワーク全体］ウィンドウが表示されます。ワークグループと同じ名前のアイコンをダブルクリックします。

4 同じワークグループのコンピュータの一覧が表示されます。P.6-309［Web Caster 800のホスト名］に設定した名前のアイコンがWeb Caster 800のファイルサーバです。アイコンをダブルクリックすると各パーティションのアイコンが表示されますのでアクセスするパーティションのアイコンをダブルクリックします。

Windows® 98/98Second Edition

1　デスクトップ上の［マイ ネットワーク］アイコンをダブルクリックします。

［ネットワークコンピュータ］ウィンドウが表示され、同じワークグループのコンピュータの一覧が表示されます。P.6-309［Web Caster 800のホスト名］に設定した名前のアイコンがWeb Caster 800のファイルサーバです。アイコンをダブルクリックすると各パーティションのアイコンが表示されますのでアクセスするパーティションのアイコンをダブルクリックします。

FTP サーバの設定

USB ストレージデバイスの最初のドライブ番号 A は FTP サーバとしても使用できます。FTP サーバとして使用した場合はインターネットから USB ストレージデバイスにアクセスしてファイルのアップロードやダウンロードが出来るようになります。
FTP サーバを使用するためには FTP サーバ用のユーザアカウントの作成とユーザホームディレクトリの作成が必要になります。

FTP ユーザアカウントの作成

1 サイドバーから［カスタム設定］アイコンをクリックします。

2 ［カスタム設定］画面が表示されます。［ユーザ］アイコンをクリックします。

3 **［ユーザ］設定画面が表示されます。［ユーザの追加］の［追加］ボタンをクリックします。**

4 **［ユーザ］設定画面が表示されます。****P.6-301「ログインユーザ名・ログインパスワード設定」の［ユーザの新規作成］の手順****で、フルネーム、ユーザ名、パスワードを設定します。**

5 **［OK］ボタンをクリックします。アカウントが作成され［ユーザ］設定画面に戻ります。**

! ご注意

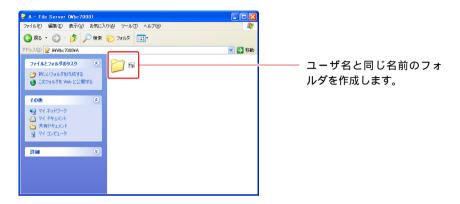
［権限］は設定する必要がありませんが、作成したアカウントに他の機能の権限を与える場合には必要な権限にチェックを入れてください。

FTP ユーザホームディレクトリの作成

1 **マイネットワーク上に［File Server］アイコンが表示されます。ファイルサーバに作成してあるパーティションのうち、一番ドライブ番号が若いパーティション（通常は A）のアイコンをダブルクリックします。**

2 **ユーザ名の入力を求められますので、ファイルサーバに書き込み権限のあるユーザアカウントのユーザ名とパスワードを入力して［OK］ボタンをクリックします。**

3　ファイルサーバにアクセス出来るようになります。

4　ファイルサーバに作成したFTPアカウントのユーザ名と同じ名前のフォルダを作成します。

ご注意

フォルダ名はユーザアカウントと必ず同じ名前にしてください。大文字と小文字は区別されますので、大文字と小文字を間違えないようにしてください。

5　作成したフォルダが自動的にFTPアカウントのホームディレクトリになります。複数のアカウントを作成する場合は、作成したアカウントごとにホームディレクトリを作成します。

リモートアクセスの設定

FTP サーバにインターネットからアクセスする場合にはリモートアクセスの設定を行う必要があります。

1 **サイドバーから［セキュリティ設定］アイコンをクリックします。**

2 **［セキュリティ設定］画面が表示されます。［リモートアクセス］ボタンをクリックします。**

3 ［リモートアクセス設定］画面が表示されます。［FTP サーバを外部に公開する］にチェックを入れ、［OK］ボタンをクリックします。

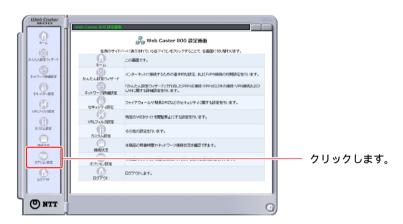
4 FTP サーバがインターネット上に公開されますので、FTP クライアントソフトを使用してインターネット上から Web Caster 800 の WAN 側の IP アドレスまたはダイナミック DNS で設定した URL にアクセス出来るようになります。

! ご注意

日本語ファイル名を表示する場合は UTF-8 をサポートした FTP クライアントをご利用ください。

FTP サーバへの anonymous 設定

本商品は USB ストレージを使用した FTP サーバへの anonymous ログインに対応しています。 なお、anonymous ログインを許可するためには、“ anonymous ” というディレクトリを FTP サーバが動作するストレージ（USB ストレージの最初のパーティション）の “ / ”（ルート）ディレクトリに事前に作成しておく必要があります。
anonymous ユーザは、このディレクトリ内のみ接続することができます。

1 サイドバーから［オプション設定］アイコンをクリックします。

2 ［オプション設定］画面が表示されます。［FTPサーバ］アイコンをクリックします。

3　**［FTPサーバ］の画面が表示されます。**
［FTP サーバへの anonymous ログインを許可する］にチェックします。

4　**［OK］ボタンをクリックします。**

Web サーバの設定

USB ストレージデバイスに作成した各パーティションは Web サーバとしても使用できます。Web サーバとして使用する場合は各パーティションに HTML ファイルをコピーすることでインターネット上に Web ページを公開できるようになります。

お知らせ

- 画面表示はお使いのパソコンにより一部異なる場合があります。
- 追加機能パッケージ「PHP 対応 Web サーバ」をインストールすることにより、PHP 対応 Web サーバをご利用になることができます。PHP 対応 Web サーバについてはP.6-284の「PHP 対応 Web サーバの機能」をご覧ください。

リモートアクセスの設定

1 サイドバーから［セキュリティ設定］アイコンをクリックします。

2 ［セキュリティ設定］画面が表示されます。［リモートアクセス］ボタンをクリックします。

3　**[リモートアクセス設定] 画面が表示されます。[Webサーバを外部に公開する(TCPポート80)] にチェックを入れ、[OK] ボタンをクリックします。**

4　**Webサーバがインターネット上に公開されます。Webブラウザでアクセスするときは、「http://Web Caster 800のアドレス/ドライブ番号(A～Z)/ファイル名」をWebブラウザのアドレスまたは場所に入力してください。**

ご注意

[Web Caster 800のアドレス] はWeb Caster 800のWAN側のIPアドレスまたはダイナミックDNSに登録しているアドレス(ダイナミックDNS使用時)を入力します。
[ドライブ番号(A～Z)] はアクセスしたいパーティションのドライブ番号です。
[ファイル名] はWebブラウザに表示させたいHTMLファイルです。パーティションにインデックスファイル(index.htmまたはindex.html)がある場合はファイル名の入力を省略できます。

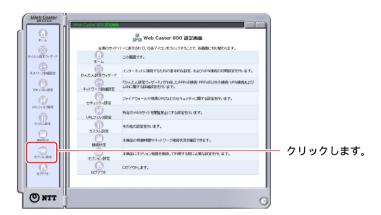
ダイナミック DNS の設定

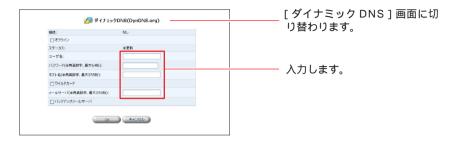
Web サーバなどをインターネットに公開するときは、固定のグローバル IP アドレスが本商品に割り当てられている必要があります。しかし、インターネットに常時接続していても切断、再接続の際に動的に IP アドレスが変ってしまう場合があります。
ダイナミック DNS を使用すると、本商品の IP アドレスをダイナミック DNS サーバに一定間隔で通知することで、IP アドレスが変わった場合でも固定のホスト名が使用できます。

お知らせ

- 本商品は DynDNS.org および DP-21.NET のダイナミック DNS に対応しています。本商品のダイナミック DNS の設定を行う前に、各サービスへの登録を行ってください。
- DynDNS.org の一部機能は、無償で提供されています（2004 年 5 月現在）。詳しくは DynDNS.org のサイト「http://www.dyndns.org/」をご覧ください。
- DP-21.NET は有償で提供されています（2004 年 5 月現在）。詳しくは DP-21.NET のサイト「http://www.dp-21.net/」をご覧ください。
- プロバイダによっては本設定をしなくても、ダイナミック DNS サービスを利用できる場合があります。詳しくはご利用のプロバイダにお問い合せください。

ダイナミックDNS(DynDNS.org)の設定

1 **サイドバーから［オプション設定］アイコンをクリックします。**

2 **［ダイナミックDNS（DynDNS.org)］アイコンをクリックします。**

3　ダイナミックDNSサービスに登録した内容をもとに各項目を入力します。

[接続]
ダイナミックDNS（DynDNS.org）へ関連付けるPPPoEの接続名を選択します。

[オフライン]
ダイナミックDNS（DynDNS.org）の更新をとめるときチェックを付けます。

[ステータス]
現在の更新情報が表示されます。

[ユーザ名]
ダイナミックDNS（DynDNS.org）に登録されているユーザ名を入力します。

[パスワード]
ダイナミックDNS（DynDNS.org）に登録されているユーザパスワードを入力します。

[ホスト名]
ダイナミックDNS（DynDNS.org）に登録されているホスト名を入力します。例えばホスト名が、webcaster.dyndns.orgの場合なら「webcaster.dyndns.org」と、完全なホスト名を入力する必要があります。

[ワイルドカード]
サブドメイン名をエイリアス設定するか指定します。チェックを付けると有効になります。
有効：例えばホスト名がwebcaster.dyndns.orgの場合なら、www.webcaster.dyndns.orgや、ftp.webcaster.dyndns.orgなどのサブドメインも、同じIPアドレスで運用が出来ます。
無効：サブドメインのワイルドカードエイリアスは設定せず、指定したホスト名だけを運用したい場合です。

[メールサーバ]
登録したドメイン宛のメールの転送先メールサーバをホスト名で指定します。

[バックアップメールサーバ]
メールサーバを入力した場合のみ、バックアップメールサーバの設定を行います。チェックを付けると有効になります。
有効：[ホスト名]で入力したホストを優先して利用した場合です。セカンダリメールサーバには[メールサーバ]で入力したホストが設定されます。MX preferenceはそれぞれ5と10になります。

無効：[メールサーバ]を入力していない場合や、[メールサーバ]で入力したメールサーバのみ利用する場合です。[メールサーバ]で入力したメールサーバのMX preferenceは10になります。

---

4 **［OK］ボタンをクリックします。**

5 **以上で設定は終了です。**
設定が完了するとダイナミックDNSサーバへ本商品が取得しているIPアドレスを定期的に通知するようになります。

ダイナミックDNS（DP-21.NET）

DP-21.NETダイナミックDNSサービスを利用する場合に設定します。

1　サイドバーから［オプション設定］アイコンをクリックします。

2　［ダイナミックDNS（DP-21.NET）］アイコンをクリックします。

3 ダイナミック DNS サービスに登録した内容をもとに各項目を入力します。

[有効にする]
設定を有効にする場合チェックします。

[ユーザ名（半角英数字、最大 64 桁）]
あらかじめ登録してあるユーザ名を入力します。

[パスワード（半角英数字、最大 64 桁）]
パスワードを入力します。

[更新間隔]
グローバル IP アドレスの更新間隔を選択します。

4 ［OK］ボタンをクリックします。

5 以上で設定は終了です。
設定が完了すると DP-21.NET ダイナミック DNS サーバへ本商品が取得している IP アドレスを定期的に通知するようになります。

IPv6ブリッジ設定

本商品はIPv6ブリッジ機能に対応しています。本機能を利用することでIPv6プロトコルを利用したパケットについて、WAN-LAN間の通信データを全てブリッジすることができます。

これにより、通常のPPPoEによるインターネット接続等とIPv6ネットワークをLAN側に設置されたパソコンで同時にご利用頂くことが可能となります。

※パソコンのIPv6設定については、お使いのパソコン及びOSの取扱説明書等をご覧ください。

IPv6ブリッジ機能の設定

1 サイドバーから［カスタム設定］アイコンをクリックします。

2 ［カスタム設定］の画面が表示されます。［IPv6ブリッジ］アイコンをクリックします。

3 ［IPv6 ブリッジを有効にする］にチェックがついているのを確認します。
本商品のIPv6 機能を無効にする場合は、チェックを外します。

4 ［OK］ボタンをクリックします。

5 以上で設定は終了です。

! ご注意

IPv6 ブリッジはデフォルト有効です。

PPPoE ブリッジ機能の設定

本商品は PPPoE ブリッジ機能に対応しています。本機能を利用することで、LAN 側に接続したパソコンが直接 PPPoE 接続して通信することができます。本機能を利用してパソコンに直接グローバルアドレスを割り当てることによって、NAT によるアドレス変換を行うことで使用できないアプリケーションが使用できるようになります。
本機能を用いて最大 2 セッションの PPPoE 接続を行うことができます。また、同時に本商品による PPPoE 接続も最大 4 セッションまで利用できます。

※パソコンの PPPoE 接続の設定については、お使いのパソコン及び OS の取扱説明書等をご覧ください。

PPPoE ブリッジ機能の設定

1 サイドバーから［カスタム設定］アイコンをクリックします。

2 ［カスタム設定］の画面が表示されます。［PPPoE ブリッジ］アイコンをクリックします。

3 **［PPPoE ブリッジ］を有効にするチェックがついているのを確認します。本商品の PPPoE ブリッジ機能を無効にする場合は、チェックを外します。デフォルトは無効なので、［PPPoE ブリッジを有効にする］にチェックをつけます。**

4 **［OK］ボタンをクリックします。**

5 **以上で設定は終了です。**

! ご注意

PPPoE ブリッジ機能はデフォルトで無効となっています。ご利用の際に設定するようにしてください。

追加機能パッケージ

本商品では、各種の追加機能を「追加機能パッケージ」として提供します。
当社ホームページからダウンロードした追加機能を、本商品にインストールすることで新機能をご利用いただけます。
また、インストールした「追加機能パッケージ」は各パッケージごとに、有効／無効の切り替えが可能です。

「追加機能パッケージ」のインストール

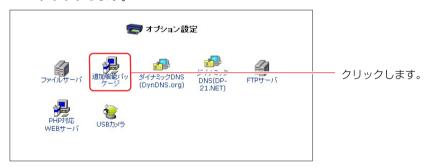
「追加機能パッケージ」のインストールを開始する前に、「追加機能パッケージ」ファイルをダウンロードして、パソコンのハードディスク上に保存しておいてください。

お知らせ

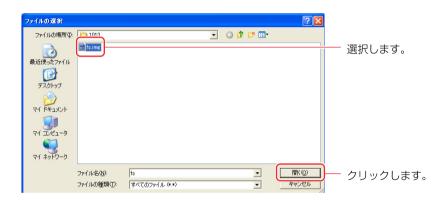
「追加機能パッケージは」以下の弊社ホームページに掲載しております。
http://www.ntt-east.co.jp/ced/
http://www.ntt-west.co.jp/kiki/

追加機能パッケージのインストール

1 **サイドバーから［オプション設定］アイコンをクリックします。**

2 **［オプション設定］画面が表示されます。［追加機能パッケージ］アイコンをクリックします。**

3 **［追加機能パッケージ］設定画面が表示されます。［パッケージのインストール］ボタンをクリックします。**

4 ［パッケージのインストール］画面が表示されます。［参照］ボタンをクリックします。

5 ファイルを選択するダイアログボックスが表示されます。保存しておいた［追加機能パッケージ］ファイルを選択し、［開く］ボタンをクリックします。

6 ［OK］ボタンをクリックします。

7 **[追加機能パッケージファイルのダウンロードに成功しました] の画面が表示されます。[OK] ボタンをクリックすると、追加機能パッケージを本商品にインストールします。**

8 **「追加機能パッケージ」のインストールが開始されます。インストールが終了すると [追加機能パッケージ] 設定画面が表示されます。画面にインストールされた「追加機能パッケージ」が一覧表示されます。**

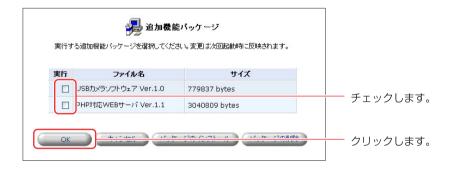
「追加機能パッケージ」の設定

インストールした「追加機能パッケージ」は、各パッケージごとに「有効」または「無効」に設定することができます。

1 **サイドバーから[オプション設定]アイコンをクリックします。**

2 **[オプション設定]画面が表示されます。[追加機能パッケージ]アイコンをクリックします。**

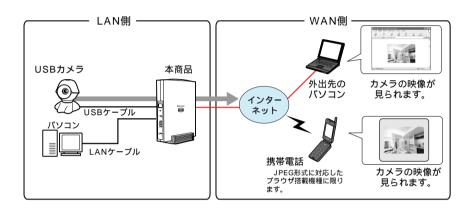
3 **[追加機能パッケージ] 設定画面が表示されます。画面にインストールされた「追加機能パッケージ」が一覧表示されます。チェックボックスにチェックされたパッケージが「有効」に設定されているパッケージです。**

4 **「有効」に設定したいパッケージのチェックボックスをチェックします。「無効」に設定したいパッケージのチェックボックスはチェックを外します。**

5 **[OK] ボタンをクリックします。**

! ご注意

本商品にインストールした追加機能パッケージを有効にする場合は再起動が必要になります。

USBカメラサーバの設定

本商品のUSBインタフェースに接続したUSBカメラ（別売）で撮影した静止画や動画を、リモートアクセスしたPCや携帯電話で見ることができます。
ここでは、USBカメラを有効にする設定と画像を見る方法について説明します。
本体に接続できるUSBカメラは1台のみです。

※本商品へのUSBカメラ接続方法は、USBカメラ「EE260」の取扱説明書をご参考ください。

※事前に、追加機能パッケージ「USBカメラソフトウェア」がインストールされていて、有効となっていることをご確認ください。追加機能パッケージのインストールについては、P.6-268の「追加機能パッケージ」をご覧ください。

※事前に、カメラ画像を見るユーザを登録して、[USBカメラ]を見る権限を設定する必要があります。ユーザの登録および権限の設定については、P.6-301の「ログインユーザ名・ログインパスワード設定」をご覧ください。

USB カメラ設定

1 サイドバーから［オプション設定］アイコンをクリックします。

2 ［オプション設定］画面が表示されます。［USB カメラ］アイコンをクリックします。

「USB カメラ]アイコンが表示されない場合は、追加機能パッケージがインストールされているかご確認ください。

3 ［USBカメラ］設定画面が表示されます。本商品にUSBカメラ接続後、「オン］にチェックをつけます。

お知らせ

「USBカメラ」設定画面の[オン／オフ]は、デフォルトの設定が[オフ]になっています。

お願い

USBカメラを取り外す場合は、「USBカメラ」を[オフ]にして、[OK]ボタンを押してから、取り外してください。

4 ［画像ビットレート］から［高（512Kbps)］または［低（128Kbps)］のいずれかを選択します。

5 ［OK］ボタンをクリックします。

USBカメラの撮影とストリーミングの画像の配信が自動的に始まります。

※この状態で、LAN内のパソコンから、USBカメラの画像を見ることが出来ます。パソコンから見る方法については、P.6-280の「パソコンで画像を見る」をご覧ください。

インターネットからカメラ画像を見る場合

ここでは、インターネットからカメラ画像を見るための設定方法について説明します。

※事前に LAN 内のパソコンから、USB カメラ画像を見ることができることをご確認ください。

1 **サイドバーから［セキュリティ設定］アイコンをクリックします。**

2 **［セキュリティ設定］画面が表示されます。［リモートアクセスボタンをクリックします。**

3 ［リモートアクセス設定］画面が表示されます。
［WEB サーバを外部に公開する（プライマリポート 80）］または［WEB サーバを外部に公開する（セカンダリポート 8080）］の使用していないポート番号の方にチェックします。また、［USB カメラ画像を外部に公開する（TCP ポート 8090）］にもチェックをつけます。

4 ［OK］ボタンをクリックします。

5 以上で設定は終了です。

※事前に LAN 内のパソコンから、USB カメラ画像を見ることができます。
パソコンから見る方法については P.6-280「パソコンから画像を見る」をご覧ください。

パソコンや携帯電話で画像を見るための条件

USB カメラで取り込んだ画像を PC や携帯電話で見る場合、PC や携帯電話の種類によって以下のソフトウェアや条件が必要となります。

端末	静止画サイズ	動画サイズ	必要なソフトウェア・条件
Windows®	320×240	320×240	Microsoft®Internet Explorer4.0以上 Netscape Navigator®6.0以上 Microsoft®Windows®Media Player7.0以上
Macintosh®	320×240	320×240	Microsoft®Internet Explorer4.0以上 Netscape Navigator®6.0以上 Microsoft®Windows®Media Player Mac板 （Windows®Media Player for Mac OS® X, Windows®Media Player 7.1 for Mac OS®8-9
Linux	320×240	320×240	Netscape Navigator®6.0以上 Mplayerなど
携帯電話	112×96	なし	JPEG画像をサポートしている機種のみ。 機種によっては利用できない場合があります。

パソコンで画像を見る

本商品にパソコンからリモートアクセスして、画像を見る方法について説明します。

1　ブラウザから、URL を指定します。

- **インターネットからアクセスする場合**
  「http://WAN 側 IP アドレス/cam/」
- **LAN からアクセスする場合**
  「http://LAN 側 IP アドレス/cam/」

ワンポイント

WAN 側 IP アドレスは、通常 PPPoE を接続する毎に変わりますが、インターネットから USB カメラ画像を見るためには、変更された WAN 側 IP アドレスに対してアクセスしなければなりません。
ダイナミック DNS サービスを使用することにより、設定したホスト名にアクセスして USB カメラ画像の閲覧などが可能となります。
「http://ホスト名/cam/」
ただし、変更された WAN 側 IP アドレスが反映されるのに時間を要する場合があり、USB カメラにアクセスすることができないことがあります。
ダイナミック DNS サービスについては、P.6-258 の「ダイナミック DNS の設定」をご覧ください。

2　本商品にリモートアクセスすると、ログイン認証を行ないます。事前に登録したログインユーザ名とログインパスワードを入力して、［OK］ボタンをクリックしてください。

お知らせ

このログイン認証機能は、撮影された画像・動画を特定の相手にのみ公開することを完全に保証するものではありません。

3 **ログイン認証終了後、[Web Caster 800・ライブカメラ] 画面が表示されます。画面にあるメニューから、観覧するカメラ画像の種類を選択します。**

[カメラ画像・静止画]
クリックすると静止画のページを表示します。

[カメラ画像・動画]
クリックすると動画のページを表示します。

[カメラページトップ]
このメインページを表示します。

メニュー項目を選択することで、どの画面からでも随時切り替えることできます。

4 ［カメラ画像・静止画］を選択した場合、「ライブカメラ静止画像」画面が表示されます。［更新］ボタンをクリックすると、現在の画像を更新します。

※画像ははめ込み合成です。

5 ［カメラ画像・動画］を選択した場合、「ライブカメラ動画」画面が表示されます。

※画像ははめ込み合成です。

ご注意

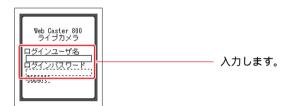
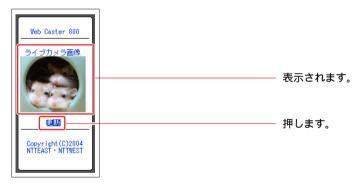
- 動画配信の場合、ネットワークの状況やWindows® Media Playerのバッファリング処理等のため、画像が表示されるまでに時間がかかる場合があります。
- 動画、静止画ともに画像の輝度、コントラストなどの調整を行うことはできません。

携帯電話で画像を見る

本商品に携帯電話からリモートアクセスして、画像を見る方法について説明します。

1 **携帯電話のブラウザから、URLを指定してリモートアクセスします。**

・携帯電話用アドレス：http://WAN側アドレス/i/

2 **本商品にリモートアクセスすると、ログイン認証を行ないます。すでに登録してあるユーザ名とパスワードを入力してください。**

3 **ログイン認証終了後、画像表示用のメインページが表示されます。[更新]ボタンを押すと、現在の画像を更新します。**

※画像ははめ込み合成です。

お知らせ

- **画像の輝度やコントラストなどの調整を行うことはできません。**
- **動作可能な携帯電話端末については、下記のWeb Caster 800のサイト上で随時公開しています。**
  http://www.ntt-east.co.jp/ced/　（NTT東日本）
  http://www.ntt-west.co.jp/kiki/　（NTT西日本）

PHP 対応 Web サーバ機能

ここでは、本商品の PHP 対応 Web サーバを WAN 側に公開する方法について説明します。
本商品で PHP スクリプトを動作させる場合は、本商品に接続された USB ストレージ（ハードディスク、フラッシュメモリ等）に PHP スクリプトを配置することで、表示が可能になります。

また、配置した PHP スクリプトを WAN 側から見る場合は、PHP スクリプトを配置した USB ストレージのディレクトリ、パーティション設定を行い、8008 番ポートをパケットフィルタリングで通過させます。

! ご注意

本商品の 80 番、8080 番ポートを利用した Web サーバ公開の設定に関しましては、従来と同じ設定方法でご利用できます。

PHP 対応 Web サーバのルートディレクトリ設定

1　**サイドバーから [オプション設定] アイコンをクリックします。**

2 ［オプション設定］画面が表示されます。［PHP 対応 WEB サーバ］アイコンをクリックします。

3 ［PHP 対応 WEB サーバ］画面が表示されます。［パーティション］欄から PHP スクリプトを配置するパーティションを選択します。

USB ストレージをご利用の場合に、パーティション欄において、パーティションの番号（A ～ N）を選択していただくことにより、Web サーバにアクセスする時の URL を指定する際にパーティション の番号の記述を省略できます。「指定無し」を選択した場合には、Web サーバにアクセスする時の URL を指定する際にパーティションの番号の記述が必要となります。

※ Web サーバにアクセスする時の URL 指定の詳細については、P.6-289「インターネットから Web ページを見る場合」を参照してください。

4 ［ドキュメントルート］欄にディレクトリ名を入力し、［OK］ボタンをクリックします。

例）　・パーティションAドライブにhtmlフォルダを作成した場合

・パーティションAドライブにhtmlフォルダを作成し、その中にmainフォルダを作成した場合

USBストレージをご利用の場合に、ドキュメントルート欄において、ディレクトリ名を入力した場合には、Webサーバにアクセスする時のURLを指定する際にドキュメントルートとして指定したディレクトリの記述を省略できます。
ディレクトリ名を入力しない（空欄）場合には、Webサーバにアクセスする時のURLを指定する際にルートディレクトリ以下のディレクトリを記述してください。

例えば、“ www ” ディレクトリの中の ” html ” ディレクトリをドキュメントルートとして指定する場合は、“ www ／ html ” と入力してください。

※ Webサーバにアクセスする時のURL指定の詳細については、P.6-289「インターネットからWebページを見る場合」を参照してください。。

PHP 対応 Web サーバのインターネット公開設定

初期状態では 8008 番ポートへのインターネットからのアクセスは、パケットフィルタにより制限されています。インターネット側から PHP 対応 Web サーバにアクセスを許可するためには、以下の設定を行う必要があります。

1　サイドバーから［セキュリティ設定］アイコンをクリックします。

2　［リモートアクセス］ボタンをクリックします。

3 **［オプション設定］欄から［PHP対応WEBサーバを外部に公開する（TCPポート8008）］にチェックをつけます。**

4 **［OK］ボタンをクリックします。**

5 **以上でPHP対応Webサーバのインターネット公開設定は終了です。**

インターネットからWeb ページを見る場合

本商品のPHP対応Webサーバに設置したファイルをインターネットから接続して見る場合は、設定した内容により指定するURLが異なります。

1　パーティション指定無しドキュメントルートディレクトリ指定無しの場合

USBストレージデバイスが接続されている場合は、各パーティション番号(A～N)をディレクトリの冒頭に記述することで、各パーティションのルートディレクトリを参照することが出来ます。

http://WebCaster800のWAN側IPアドレス:8008/
パーティション番号/ルートディレクトリ以下のディレクトリ及びファイル名

（例）パーティションAのルートに“ webpage ”ディレクトリを作成し、
その中に“ index．html ”ファイルを設置した場合
http://＊＊＊.＊＊＊.＊＊＊.＊＊＊：8008/A/webpage/

2　パーティション番号のみ指定した場合

USBストレージデバイスをご利用の場合に、指定したパーティションのルートディレクトリをドキュメントルートとして参照することが出来ます。

http://WebCaster800のWAN側IPアドレス:8008/
ルートディレクトリ以下のディレクトリ及びファイル名

（例）“ パーティションとして“ A ”を指定し、パーティションAのルートに“ webpage ”ディレクトリを作成し、その中に“ index.html ”
http://＊＊＊.＊＊＊.＊＊＊.＊＊＊:8008/webpage/index.html

3　ドキュメントルートのみ指定した場合

指定したディレクトリをドキュメントルートとして参照することが出来ます。

・USB ストレージデバイスをご利用の場合

USB ストレージデバイスをご利用の場合は、ドキュメントルート欄に参照するパーティション番号を記述する必要があります。
http://WebCaster800 の WAN 側 IP アドレス:8008/
ドキュメントルート以下のディレクトリ及びファイル名

（例）ドキュメントルートとして " webpage " を指定し、パーティション A のルートに " webpage " ディレクトリを作成し、その中に " index.h tml " ファイルを設置し、ドキュメントルート欄に［A/web page］と記述した場合
http://＊＊＊.＊＊＊.＊＊＊.＊＊＊:8008/index.html

4　パーティション番号およびドキュメントルートを指定した場合

USB ストレージデバイスをご利用の場合に、指定したパーティションの指定したディレクトリをドキュメントルートとして参照することが出来ます。

http://WebCaster800 の WAN 側 IP アドレス:8008/
ドキュメントルート以下のディレクトリ及びファイル名

（例）パーティションとして" A "、ドキュメントルートとして" webpage " を指定し、パーティション A のルートに" webpage "ディレクトリを作成し、その中に" index.html "ファイルを設置した場合
http://＊＊＊.＊＊＊.＊＊＊.＊＊＊:8008/index.html

PHP スクリプト動作機能

PHP 対応 Web サーバのパッケージ追加を行うことにより、コマンドライン上でユーザが作成した任意の PHP スクリプトが動作します。本商品に接続した USB ハードディスク上で実行することが出来ます。

ご注意

本商品が対応しているスクリプトは PHP スクリプトのみになります。
・スクリプトには、インタプリタ起動用として 1 行目に
“ #/usr/local/bin/php［改行］” と記述する必要があります。
・文字コードには、2 バイト文字は使えません。
・改行コードは “ LF ” を使用してください。
・ root 権限での実行は出来ません。一般ユーザ権限で使用してください。

telnet接続機能

PHP対応Webサーバのパッケージ追加を行うことにより、コマンドライン上でユーザが作成した任意のPHPスクリプトが動作します。本商品に接続したUSBハードディスク上で実行することが出来ます。

ご注意

PHPスクリプトの実行等の操作を簡単に行うため、1023番ポートに対してLAN側からtelnetによる接続を行い、シェルを利用することが可能です。

・1023番で接続するとユーザ名/パスワードの認証が行われます。
・管理者権限ユーザ以外でログインすることが可能です。
・ログインすると、/home/httpd/htmlというディレクトリに入ります。その後、“ cd ”コマンドで実際に操作するパーティション名に移動し、コマンドを実行してください。

例）

```
/home/httpd/html $ cd A<enter>
/home/httpd/html/A $ ./test.php<enter>
```

スタートアップスクリプト機能

ユーザが作成したPHPスクリプトを自動起動させる機能です。USBハードディスクのルートディレクトリ上に“startup”というファイルが存在した場合、本商品の起動時にそのファイルを自動的に実行します。
起動時に、USBハードディスクの各パーティションのルートディレクトリを検索し、“startup”というファイルが存在した場合には全て実行します。

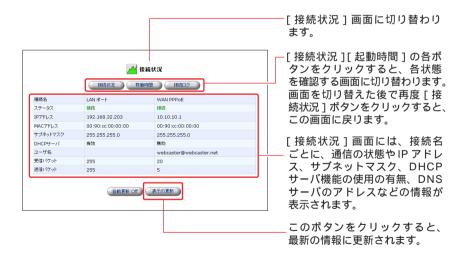
保守・管理

本商品の運用開始後にネットワークの接続状態の確認や、管理者のログイン名やパスワードの変更方法などを説明します。

機器状況の確認

接続状態の確認

各接続ポートごとに通信状態やアドレス情報等が確認できます。

1　サイドバーから［接続状況］アイコンをクリックします。

[WAN ポート]

PPPoE 以外の方法でインターネットに接続している場合の、WAN 側の通信の状況が確認できます。

[WAN PPPoE]

PPPoE でインターネットに接続している場合の WAN 側の通信の状況が確認できます。

[LAN ポート]

LAN ポートの通信の状況が確認できます。

[VPN PPTP]

本商品が PPTP クライアントである場合の通信の状況が確認できます。

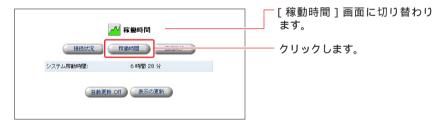
[VPN IPSec]

IPSec で通信している状況が確認できます。

稼動時間の確認

ここでは本商品が稼動してからの現在までの時間を確認できます。

1　サイドバーから［接続状況］アイコンをクリックします。

2　［稼動時間］ボタンをクリックします。

●画面表示の自動更新を停止する
［カスタム設定］画面－［システム設定］画面で［システムモニタページの表示の自動更新を行う］をチェックしているときは、［接続状況］の各画面は一定間隔で自動更新されます。このとき、［接続状況］の各画面の［自動更新 Off］ボタンをクリックすると、［今すぐ更新］ボタンをクリックした時のみ、［接続状況］の各画面の内容が更新されるようになります。

接続ログの確認

ここでは、PPPoE 接続、VPN 接続のネットワークへの接続状態の確認をする方法について説明します。

接続ログの確認

1 **サイドバーから［接続状況］アイコンをクリックします。**

2 ［接続状況］の画面が表示されます。［接続ログ］ボタンをクリックします。

接続名	LANポート	WAN PPPoE	WAN PPPoE 2
ステータス	接続	接続	接続
MACアドレス	00:90:cc:61:8b:b4		
IPアドレス	192.168.1.1	221.184.88.29	220.216.188.48
サブネットマスク	255.255.255.0		
デフォルトゲートウェイ		61.207.30.50	220.210.195.68
DNSサーバ		202.234.232.223 211.129.12.214	220.210.194.67 220.210.194.68
DHCPサーバ	有効		
ユーザ名		f09s2jus@ipcon.ocn.ne.jp	guest@flets
受信パケット	783	7	3
送信パケット	1236	5	3
トータルパケット	2019	12	6

クリックします。

3 本商品の接続ログが表示されます。

時刻	イベント	タイプ	詳細
Dec 16 15:25:39 2003	System Log	Message	local2.notice pppd[83]: secondary DNS address 220.210.194.68
Dec 16 15:25:39 2003	System Log	Message	local2.notice pppd[83]: primary DNS address 220.210.194.67
Dec 16 15:25:39 2003	System Log	Message	local2.notice pppd[83]: remote IP address 220.210.195.68
Dec 16 15:25:39 2003	System Log	Message	local2.notice pppd[83]: local IP address 220.216.188.48

ログの見方（例）

詳細メッセージ	説明
Sending PADI	PPPoE セッションが開始されました。
Connection-Terminated	セッションが終了しました。
Authentication-failuer	認証に失敗しました。
Rejecting IP Address	PPPoE サーバから IP アドレスが拒否されました。
local IP address	WAN ポートの IP アドレスを取得しました。
remote IP address	デフォルトゲートウェイの IP アドレスを取得しました。
primary DNS address	プライマリ DNS サーバの IP アドレスを取得しました。
secondary DNS address	セカンダリ DNS サーバの IP アドレスを取得しました。
listening for IKE messages	IKE メッセージを確認しています。
initiating Main mode	IPsec のメインモードを開始しました。
ISAKMP SA established	メインモードで ISAKMP SA を確立しました。
initiating Quick mode	IPsec のクイックモードを開始しました。
IPsec SA established	IPsec をメインモードで確立しました。
deleting connection	接続を切断しました。
MSCHAP-v2 peer authentication	PPTP 接続を MSCHAP-v2 で認証しました。

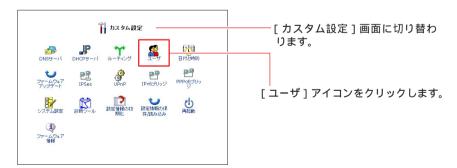
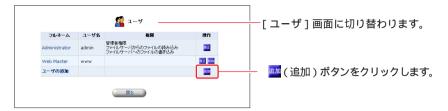
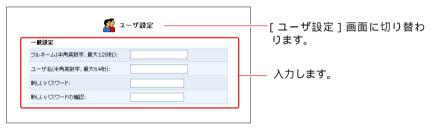
MSCHAP peer authentication	PPTP接続をMSCHAPで認証しました。
CHAP peer authentication	PPTP接続をCHAPで認証しました。
MPPE 128bit	PPTP接続でMPPE 128bitが有効です。
MPPE 40bit	PPTP接続でMPPE 40bitが有効です。

ログインユーザ名・ログインパスワード設定

本商品のログインユーザ名とパスワードの登録、変更、または削除ができます。

ユーザの新規作成

1　サイドバーから［カスタム設定］アイコンをクリックします。

2　［ユーザ］アイコンをクリックします。

3 ［ユーザの追加］欄から「追加」ボタンをクリックします。

4 ［ユーザ設定］画面が表示されます。
フルネーム、ユーザ名、新しいパスワードを入力します。

［フルネーム］
登録するユーザのフルネームを入力します。半角英数字で 128 桁まで入力できます。

［ユーザ名］
新しく登録するユーザのログイン名を入力します。半角英数字で 64 桁まで入力できます。

［新しいパスワード］
ユーザがログイン時に使用するパスワードを入力します。半角英数字で 64 桁まで入力できます。
大文字と小文字は区別されますのでご注意ください。

［新しいパスワードの確認］
「新しいパスワード」と同じパスワードを再度入力します。

5 本商品での権限を設定します。

[管理者権限]
ユーザを管理者として登録する場合は、チェックします。

[PPTP リモートアクセス]
PPTP による VPN 接続を許可する場合は、チェックします。

[ファイルサーバからのファイルの読み込み]
USB ストレージデバイスを接続したときに、ファイル読み込みを許可する場合は、チェックします。

[ファイルサーバへのファイルの書き込み]
USB ストレージデバイスを接続したときに、ファイル書き込みを許可する場合は、チェックします。

[USB カメラ]
USB カメラのリモートアクセスページへの接続を許可する場合は、チェックします。

※ここで登録されたユーザは、FTP サーバへアクセスする際の認証アカウントに設定されます。詳細は「6 章 オプション設定」を参照してください。

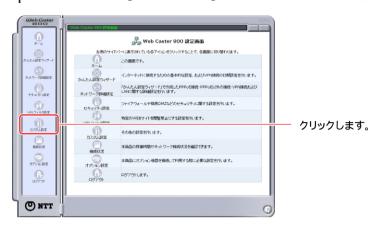
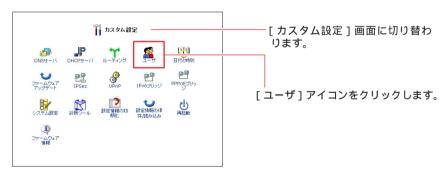
6 E-mail 通知を利用する場合は、E-mail アドレス、システム通知レベル、セキュリティ通知レベルを設定します。

※ E-mail 通知機能に関しては E-mail 通知機能をご参照ください

7 [OK] ボタンをクリックします。

8 以上で設定は終了です。

ユーザの修正

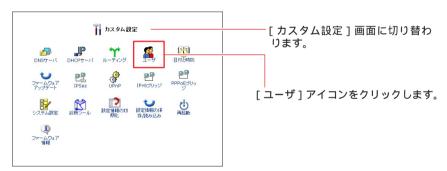
1　サイドバーから［カスタム設定］アイコンをクリックします。

2　［ユーザ］アイコンをクリックします。

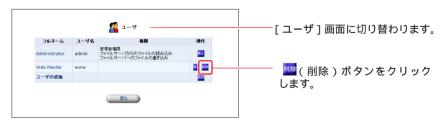
3　設定を変更したいユーザの「修正」ボタンをクリックします。

4 **［ユーザ設定］画面が表示されます。修正したい項目の変更を行い、［OK］ボタンをクリックします。**

5 **以上で設定は終了です。**

ユーザの削除

1　サイドバーから［カスタム設定］アイコンをクリックします。

2　［ユーザ］アイコンをクリックします。

3　設定を削除したいユーザの「削除」ボタンをクリックします。

! ご注意

購入時に登録されてる Administrator は削除することができません。

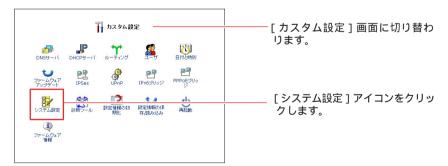
4　以上で設定は終了です。

システム設定

本商品のホスト名やLAN側のドメイン名などを設定できます。

システム設定

1 サイドバーから［カスタム設定］アイコンをクリックします。

2 ［システム設定］アイコンをクリックします。

3 ［システム］欄に本商品のホスト名、ドメイン名を入力します。

[Web Caster 800 ホスト名]
本商品のホスト名を入力します。

[ローカルドメイン]
LAN内で使用したいドメイン名を入力します。

4 ［ファイルサーバ］欄にファイルサーバを使用する際のNetBIOSワークグループ名を入力します。

[NetBIOSワークグループ]
ファイルサーバを使用する際のNetBIOSホスト名を入力します。初期値は「home」と設定されています。

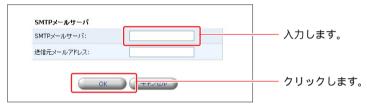
5 ［Web Caster 800設定画面］欄から［システム情報ページの表示の自動更新を行う］、［ネットワーク設定の変更時に確認を行う］を設定します。

[システム情報ページの表示の自動更新を行う]
［接続状況］画面の表示を自動的に更新させたい場合は、チェックします。

[ネットワーク設定の変更時に確認を行う]
ネットワークに関する変更をしたときに、確認メッセージを表示させたい場合は、チェックします。

6　［システムリモートログ設定］、［セキュリティリモートログ設定］を利用する場合は設定をします。

※リモートログ設定に関しては、Syslog の設定をご参照ください。

7　ユーザ設定で E-mail 通知機能を利用している場合は、［SMTP メールサーバ］欄にメールサーバのアドレスを入力します。

8　［OK］ボタンをクリックします。

9　以上で設定は終了です。

日付と時刻の設定

本商品の日付や時刻の設定を変更できます。

日付と時刻の設定

1　サイドバーから［カスタム設定］アイコンをクリックします。

2　［日付と時刻］アイコンをクリックします。

3　日付と時刻を設定します。

［日付と時刻］画面に切り替わります。

［手動設定］
日付と時刻を手動で設定します。［日付］と［時刻］を選択または入力します。

［自動設定］
日付と時刻を NTP サーバを使い、自動で設定します。

［有効］
NTP サーバから時刻を取得するときチェックを付けます。

［更新間隔］
NTP サーバへ時刻の問合せをする間隔を 1 時間から 480 時間のあいだで設定します。

［NTP サーバ］
指定された NTP サーバの IP アドレスまたはホスト名が表示されます。
NTP サーバの IP アドレスまたはホスト名は追加、修正、削除が出来ます。

［ステータス］
NTP サーバからの応答の状況が表示されます。
［サーバからの応答待ち］：設定した NTP サーバへ時刻の問合せをしています。
［時刻取得成功 最終更新：Sat Jun 1 10:00:00 2004］：NTP サーバから時刻を取得できた事と、最後に NTP サーバへアクセスした日時が表示されます。

4 **[追加]ボタンをクリックすると[NTP サーバの追加]が表示されます。追加したいNTP サーバのIP アドレスまたはホスト名を入力し[OK]ボタンをクリックします。**

5 **[OK]ボタンをクリックします。**

6 **以上で日付と時刻の設定は終了です。**

ワンポイント

NTP サーバを複数設定した場合は、登録したNTP サーバの順に時刻の問合せを行います。
NTP サーバから時刻の取得に失敗したときに次に登録したNTP サーバへ問合せを行います。
設定したNTP サーバの問合せに全部失敗してしまった場合は、[サーバからの応答待ち]の表示となります。応答があるまで約2 分間隔で問い合わせを繰り返します。

ファームウェアの更新

本商品の購入後、当社のホームページからダウンロードしたファイルを使って、最新のファームウェアにアップデートすることができます。

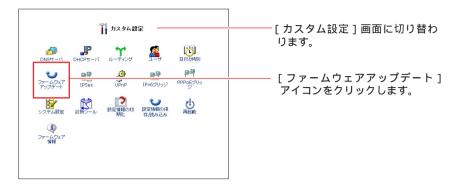
ご注意

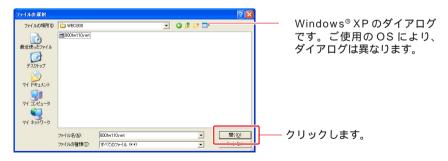
・インターネットに接続している場合は、アップデートを行う前に全ての通信を切断してください。また、LAN 内のパソコンはアップデート作業を行うパソコンを除いて全て電源を OFF にしてください。
・ファイアウォールやウィルススキャンソフトがインストールされてるパソコンでアップデート作業を行う場合は、事前にソフトウェアを終了してください。
・このアップデートは当社が独自に提供するサービスです。新機能の追加や性能の増強を保証するものではありません。

ファームウェアの更新

1 当社のホームページから最新のファームウェアをダウンロードします。
ダウンロードしたファイルは、アップデート作業を行うパソコンのハードディスクなどに保存してください。

2 サイドバーから［カスタム設定］アイコンをクリックします。

3 ［ファームウェアアップデート］アイコンをクリックします。

4 ［参照］ボタンをクリックし、ダウンロードしたファームウェアのファイルを指定します。

5 ［開く］ボタンをクリックします。

6 ［OK］ボタンをクリックすると、ファームウェアアップデートの準備が開始されます。

ご注意

ファームウェアアップデートの準備中は、絶対に Web Caster 800 の電源を切ったり、LAN ケーブルを抜いたりしないでください。ファームウェアアップデートの準備には、数十秒間かかります。［OK］ボタンをクリックしたら、そのまましばらくお待ちください。

7 ファームウェアアップデートの準備が終了すると、［ファームウェアアップデート］の画面が表示されます。
［現在のバージョン］と［新しいバージョン］に表示されるバージョン番号に間違いが無いか確認してください。
［OK］ボタンをクリックすると、ファームウェアのアップデートが開始されます。

ご注意

ファームウェアのアップデート中は、絶対に Web Caster 800 の電源を切ったり、LAN ケーブルを抜いたりしないでください。ファームウェアアップデートには、数十秒間かかります。［OK］ボタンをクリックしたら、そのまましばらくお待ちください。

8 アップデートが終了すると、本商品は自動的に再起動します。新しいバージョンのファームウェアは再起動後に有効になります。

9 再起動が完了すると、ログイン画面に戻ります。以上でファームウェアの更新は終了です。

ご注意

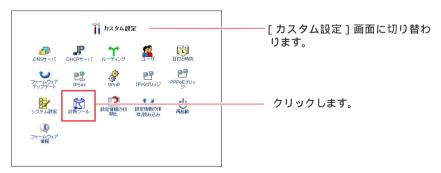
本商品以外のファームウェアを使ってアップデートを行うことはできません。無理にアップデートを行うと本商品が動作しなくなりますので、ご注意ください。

診断ツール

本商品からパソコンなどのネットワーク端末に対してPingを送信することができます。

診断ツールの使い方

1　サイドバーから［カスタム設定］アイコンをクリックします。

2　［診断ツール］アイコンをクリックします。

3 ［送信先IPアドレスまたはホスト名］欄にPingを送信したいIPアドレスまたはホスト名を入力します。

4 ［送信］ボタンをクリックすると、本商品から宛先にPingが送信されます。

5 ［ステータス］欄に送信結果が表示されます。

6 ［戻る］ボタンをクリックします。

7 以上で診断は終了です。

初期化

設定ページから本商品の設定内容を消去して、購入時の状態に戻すことができます。

※本体にあるリセットスイッチを使って、設定を消去することもできます。詳しくは本商品の取扱説明書（冊子）の「本商品を初期化する」〈P.5-10〉を参照してください。

! ご注意

この機能を使うと、設定ページにアクセスするためのパスワードを含め、変更した設定内容がすべて消去されます。また、本商品のLAN側ポートのIPアドレスを変更していた場合は、購入時の「192.168.1.1」に戻ります。ご注意ください。

本商品の初期化

1　サイドバーから［カスタム設定］アイコンをクリックします。

2　［設定情報の初期化］アイコンをクリックします。

3 ［OK］ボタンをクリックします。

［設定情報の初期化］画面に切り替わります。

［OK］ボタンをクリックします。

4 初期化が始まります。

設定内容の消去が開始します。消去中は、この画面が表示されます。

5 設定内容の消去が終わると、設定ページに初めてログインするときの画面に切り替わります。

［Web Caster 800 設定画面］に切り替わります。

［OK］ボタンをクリックします。

※画面が切り替わらないときは、［ログイン］ボタンをクリックしてください。

6 ユーザ名とパスワードを入力し、［OK］ボタンをクリックします。

［Web Caster 800 設定画面］に切り替わります。

［ログインユーザ名］
　設定ページにログインするユーザ名を入力します。

［新しいログインパスワード］
　パスワードを入力します。

［新しいログインパスワードの確認］
　［新しいログインパスワード］の内容をもう一度入力します。

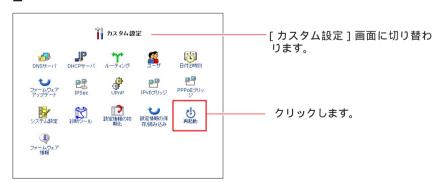
7 ［OK］ボタンをクリックすると、設定ページの［Web Caster 800 設定画面］に切り替わります。

再起動

本商品の再起動を行います。

本商品の再起動

1 サイドバーから［カスタム設定］アイコンをクリックします。

2 ［再起動］アイコンをクリックします。

3 ［OK］ボタンをクリックします。

4 再起動が完了すると、ログイン画面に切り替わります。

ファームウェア情報

本商品のファームウェアのバージョンを確認できます。

ファームウェア情報の確認

1　サイドバーから［カスタム設定］アイコンをクリックします。

2　［ファームウェア情報］アイコンをクリックします。

3　**本商品のファームウェアのバージョンが表示されます。**

4　**［戻る］をクリックします。**

設定情報の保存／読み込み機能

Web Caster 800の設定情報をコンピュータへ保存出来ます。また、保存した設定情報の読み込みが出来ます。

! ご注意

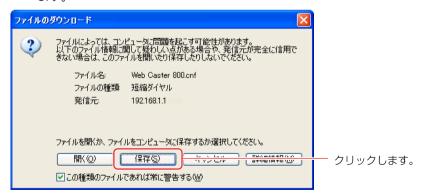
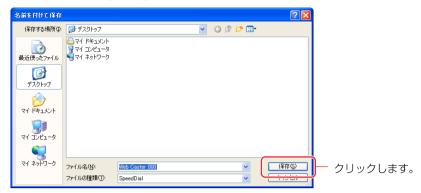
保存した設定情報は同一ファームウェアバージョンでしか読み込むことができません。今後のファームウェアのバージョンアップがあった場合には、詳細取扱説明書の設定記入シートに設定内容を記載した上で再度設定を行ってください。

設定情報の保存

1 **サイドバーから［カスタム設定］アイコンをクリックします。**

2 ［設定情報の保存/読み込み］アイコンをクリックします。

3 ［設定情報の保存］ボタンをクリックします。

4 ［ファイルのダウンロード］が表示されます。［保存］ボタンをクリックします。

5 ［名前を付けて保存］の画面が表示されます。任意の保存先およびファイル名を指定し、［保存］ボタンをクリックします。

6 以上で設定情報の保存は終了です。

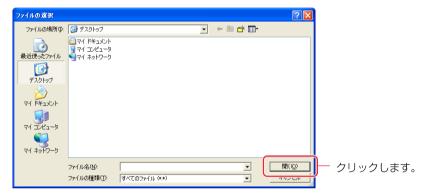
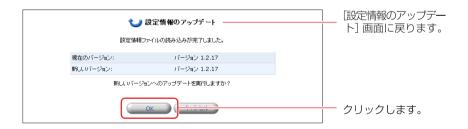
設定情報の読み込み

1　サイドバーから［カスタム設定］アイコンをクリックします。

2　［設定情報の保存/読み込み］アイコンをクリックします。

3　［［設定情報の読み込み］ボタンをクリックします。

4 ［参照］ボタンをクリックします。

5 ［ファイルの選択］の画面が表示されます。保存された設定情報を指定し、［開く］ボタンをクリックします。

6 ［設定情報の読み込み］の画面が表示されます。［OK］ボタンをクリックします。

7 ［OK］ボタンをクリックします。

8 ［システムはアップデート中です。しばらくお待ちください...］の画面が表示されます。そのまましばらくお待ちください。

9 しばらくすると［ログイン］の画面が表示されます。以上で設定情報の読み込みは終了です。

第7章 具体的な設定例

この章では、Web Caster 800の具体的な設定例について解説します。

オンラインゲームや音声/ビデオチャットを利用する

ここでは、オンラインゲームや音声/ビデオチャットを行うときに必要な設定について解説します。

UPnP に対応しているアプリケーションの場合

本商品は Universal Plug and Play（ユニバーサルプラグアンドプレイ：UPnP）に対応しています。とくに設定を行わなくても UPnP 対応のアプリケーションを利用することができます。

ご注意

- UPnP アプリケーションによっては動作しないものがあります。その場合は、そのアプリケーションの取扱説明書、サポートセンターなどでご確認ください。
- UPnP を利用できる OS は、Windows® XP および Windows® Me です。
  Windows® Me の場合は、［コントロールパネル］-［アプリケーションの追加と削除］で［ユニバーサルプラグアンドプレイ］をインストールしてください。詳しくは P.6-78「パソコンの UPnP の設定を確認する」を参照してください。

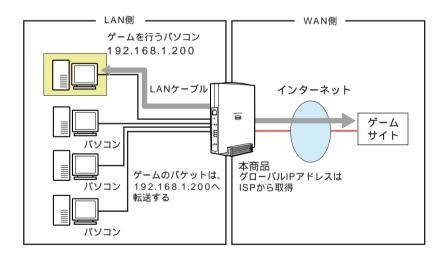
UPnP に対応していないアプリケーションの場合

オンラインゲームを使いたいときは、ゲームを行うパソコンにインターネットからのアクセスを許可する必要があります。
本商品はローカルサーバ機能に対応していますので、ローカルサーバ機能に使用するゲームのポート情報やパソコンの IP アドレスを設定するだけでご利用できます。

! ご注意

オンラインゲームを行う場合は、本商品にグローバル IP アドレスが割り当てられている必要があります。プライベート IP アドレスを利用する一部のプロバイダをご利用の場合は、オンラインゲームを行えない場合があります。グローバル IP アドレスが割り当てられているかのご確認は、ご利用プロバイダへお問い合わせください。

ここでは、LAN 内のパソコン「192.168.1.200」からオンラインゲームのサイトにアクセスし、オンラインゲームを行う場合の設定について解説します。

7
具体的な設定例

ローカルサーバを使ったオンラインゲームの設定

ここでは、本商品のローカルサーバ機能を使用してオンラインゲームとパソコンを登録する方法について説明します。

1　サイドバーから[セキュリティ設定]アイコンをクリックします。

2　[ローカルサーバ]アイコンをクリックします。

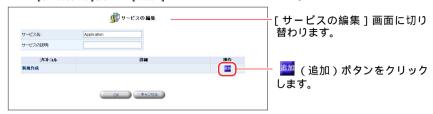
7
具体的な設定例

3 [新規作成]欄から追加ボタンをクリックします。

4 [ローカルサーバの追加]画面が表示されます。[ローカルIP]欄にゲームを行うパソコンのIPアドレスを入力します。

5 ネットワークで使用するポート情報を設定します。[ユーザ定義サービス]をクリックします。

6 [ユーザ定義サービス]画面が表示されます。[新規作成]欄から[追加]ボタンをクリックします。

7 [サービスの編集]画面が表示されます。[新規作成]欄から[追加]ボタンをクリックします。

8 [プロトコル]欄から使用するプロトコルを選択します。

[プロトコル]

対象にするプロトコルをTCP、UDPから選択します。

[発信元ポート/送信先ポート]

サービスやアプリケーションの発信元ポート/送信先ポート番号を入力します。

すべて	→全てのポートを指定します。
１個を指定	→１つのポート番号を指定します。
範囲指定	→ポート番号の範囲を指定します。

9 [OK]ボタンをクリックします。

10 追加ボタンをクリックすることで、複数のポートを指定することもできます。

11 全ての設定が終了しましたら、［サービス名］に任意の名前を入力し、[OK]ボタンをクリックします。

12 ［ユーザ定義サービス］の画面に戻ります。［サービス名］欄に作成したユーザ定義サービスが表示されているのを確認します。
［戻る］ボタンをクリックします。

! ご注意

- サービスの新規作成を行う場合は、オンラインゲームなどで使用するポート情報が必要です。詳しくはオンラインゲームのサポートセンターなどにお問い合わせください。
- 登録したいオンラインゲームのポート情報などが公開されていないときは、DMZ ホスト機能を設定してください。

13 [ローカルサーバの追加］画面に戻ります。[ユーザ定義サービス]欄に作成したユーザ定義サービスが表示されてるのを確認し、チェックを付けます。

14 [OK]ボタンをクリックします。

※[OK]ボタンは画面の下の方にあります。スクロールして表示させてください。

15 [ローカルサーバ]画面に戻ります。ローカルサーバで使用するサービスとパソコンのIP アドレスが表示されます。

16 [OK]ボタンをクリックします。

17 以上で設定は終了です。

7 具体的な設定例

Windows® Messenger、MSN® Messengerを使う

本商品とパソコンのUniversal Plug and Play（ユニバーサルプラグアンドプレイ：UPnP）機能を利用すると、Windows® Messenger Version4.7以上、MSN® Messenger5.0以上を複数台のパソコンで利用することができます。
本商品はUPnPに対応していますので、とくに設定を行う必要はありません。

! ご注意

- UPnPを利用できるOSは、Windows® XPおよびWindows® Meです。
  Windows® Meの場合は、[コントロールパネル] - [アプリケーションの追加と削除]で[ユニバーサルプラグアンドプレイ]をインストールしてください。
  詳しくは P.6-78「パソコンのUPnPの設定を確認する」を参照してください。
- 音声チャットを行うには、マイク/スピーカー、またはヘッドセットが別途必要です。
- ビデオチャットを行うには、マイク/スピーカー、またはヘッドセット、カメラ（USBカメラ）などが必要です。

利用できる機能

本商品で利用できるWindows® Messenger、またはMSN® Messenger機能は次のとおりです。

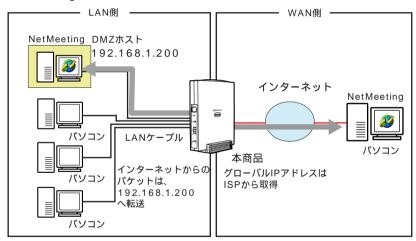
	Windows® Messenger Ver4.7以上	MSN® Messenger Ver5.0以上
インスタントメッセージ	○	○
ファイル転送	×	○
音声チャット	○	○
ビデオチャット	○	○
アプリケーション共有	○	○
ホワイトボード	○	○
リモートアシスタンス（ファイル転送機能）	○	○

NetMeeting を使う

本商品で NetMeeting を利用するときは、DMZ ホスト機能を使います。
NetMeeting は UPnP に対応しておらず、アプリケーションが使用するポートが複数あり、かつ動的にポート番号を変えながら通信を行います。このような場合は、DMZ ホスト機能を使います。

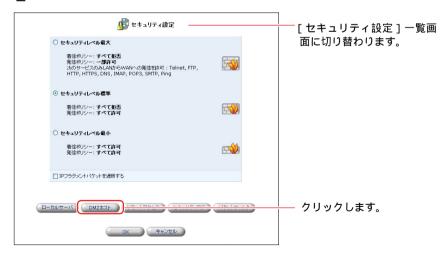
ご注意

- NetMeeting を使う場合は、本商品にグローバル IP アドレスが割り当てられている必要があります。プライベート IP アドレスを利用する一部のプロバイダではご利用できない場合があります。あらかじめご了承ください。
- LAN 内のパソコンのうち 1 台のみ、NetMeeting を使うことができます。
- DMZ ホストにはインターネットからのアクセスをすべて許可するので、外部からの攻撃を受ける可能性があります。

ここでは、LAN 内のパソコン「192.168.1.200」を DMZ ホストにして、NetMeeting を使ってチャットを行う場合の設定について説明します。

DMZ ホストを使ったNetMeetingの設定

ここでは、NetMeetingで使うパソコンをDMZホストとして設定する方法について説明します。

1　サイドバーから[セキュリティ設定]アイコンをクリックします。

2　[DMZホスト]ボタンをクリックします。

3　DMZ ホストに設定するパソコンの IP アドレスを入力し、チェックします。

4　［OK］ボタンをクリックします。

5　以上で設定は終了です。

インターネット上にサーバを公開する

ここでは、インターネット上にサーバを公開するときに必要な設定について解説します。

LAN に接続された PC をサーバとして公開する

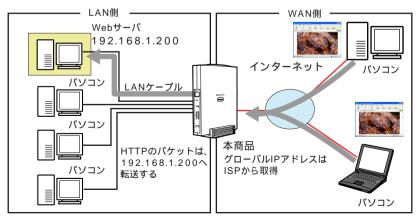
LAN 側に構築したサーバをインターネットに公開するときは、インターネットから LAN 側のサーバへのアクセスを許可する必要があります。本商品にはよく使われるインターネットのサービスがあらかじめ登録されています。サービスを選択しサーバの IP アドレスを入力すると、LAN 側のサーバをインターネットに公開できます。

! ご注意

インターネットにサーバを公開すると、外部からの侵入や盗聴、データの消失などの被害に遭う可能性があります。十分なセキュリティ設定を行ってください。

! ご注意

外部にサーバを公開する場合は、本商品にグローバル IP アドレスが割り当てられている必要があります。プライベート IP アドレスを利用する一部のプロバイダをご利用の場合は、サーバを公開できない場合があります。あらかじめご了承ください。

ここでは、LAN 側のパソコン「192.168.1.200」を Web サーバとして外部に公開する例について説明します。

ローカルサーバを使ったサービスの公開

ここでは、インターネット上に公開するサービスとパソコンのIPアドレスをローカルサーバに設定する方法について説明します。

1　サイドバーから［セキュリティ設定］アイコンをクリックします。

2　［ローカルサーバ］アイコンをクリックします。

3 ［新規作成］欄から追加ボタンをクリックします。

4 ［ローカルサーバの追加］画面が表示されます。［ローカルIP］欄にサービスを公開するパソコンのIPアドレスを入力します。

5 ［デフォルト定義サービス］欄に本商品に登録されてるサービスやアプリケーションが表示されます。ご利用になりたいサービスにチェックします。

※ Webサーバとして外部に公開する場合は、HTTP Web Serverにチェックします。

6 ［OK］ボタンをクリックします。

※［OK］ボタンは画面の下の方にあります。スクロールして表示してください。

7 ［ローカルサーバ］画面に戻ります。ローカルサーバで使用するサービスとパソコンのIPアドレスが表示されます。

8 ［OK］ボタンをクリックします。

9 以上で設定は終了です。

第8章 資料

パソコンのIPアドレスの管理や用語集などです。

パソコンの IP アドレスの管理

IP アドレスの確認

LAN 側のパソコンに設定されている IP アドレスの確認方法を解説します。

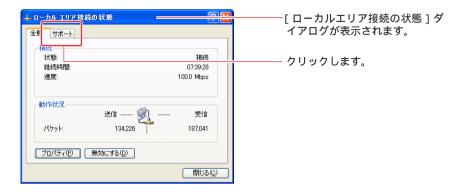
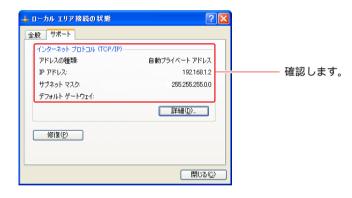
Windows® XP

ここでは、WIndows® XP の通常表示モード（カテゴリー表示モード）を前提に説明します。

1 ［スタート］メニューから［コントロールパネル］を選択し、［ネットワークとインターネット接続］を選択します。

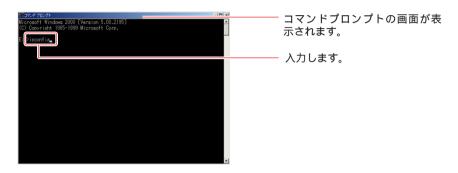
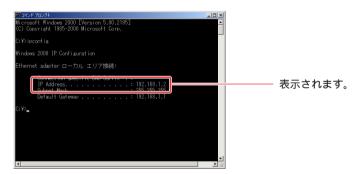
2 ［ネットワーク接続］をクリックします。

3 ［ローカルエリア接続］をクリックします。

4 ［サポート］をクリックします。

5 ［インターネットプロトコル（TCP/IP）］の［IP アドレス］欄に現在の IP アドレスが表示されます。

6 以上で IP アドレスの確認は終了です。

Windows® 2000

1 ［スタート］メニューから［プログラム］－［アクセサリ］－［コマンドプロンプト］を選択します。
コマンドプロンプトの画面が表示されます。

2 ［ipconfig］と入力し、［Enter］キーを押します。

3 使用するアダプタを選択します。［IP アドレス］欄に、現在設定されている IP アドレスが表示されます。

Windows® Me/98

ここでは、Windows® Me を例にして、現在の IP アドレスを確認します。Windows® 98 をお使いのお客さまは、同様の手順でご確認ください。

1 **［スタート］メニューから［ファイル名を指定して実行］を選択します。**

2 **［名前］欄に「winipcfg」と入力して［OK］ボタンをクリックします。**

3 **使用するアダプタを選択します。［IP アドレス］欄に、現在設定されている IP アドレスが表示されます。**

8

資料

Mac OS® X

1　画面左上のアップルメニューから、［システム環境設定］を選択します。

2　［ネットワーク］をクリックします。

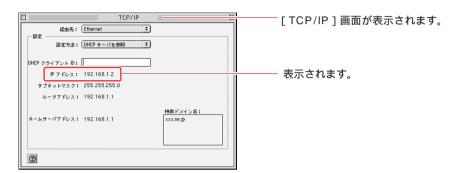
3　画面の下側が切り替わります。［IP アドレス］欄に、現在設定されている IP アドレスが表示されます。

Mac OS®（8～9）

ここでは、MacOS®9を例にして、現在のIPアドレスを確認します。他のバージョンをお使いのお客さまも、同様の手順でご確認ください。

1 **画面左上のアップルメニューから、［コントロールパネル］－［TCP/IP］を選択します。**

2 **［IPアドレス］欄に、現在設定されているIPアドレスが表示されます。**

8
資料

IP アドレスの変更

本商品の DHCP サーバ機能を利用しないで、パソコンに固定の IP アドレスを割り当てる方法を説明します。

! ご注意

パソコンに固定の IP アドレスを割り当てるときは、設定する IP アドレスにご注意ください。誤った IP アドレスを設定してしまうと、LAN 側の他の端末やインターネットと通信できなくなることがあります。

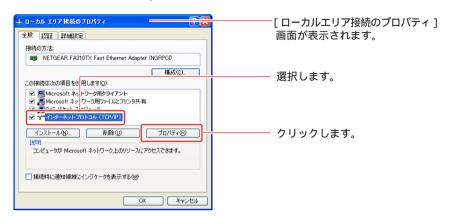
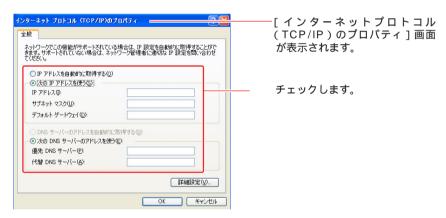
Windows® XP

ここでは、WIndows® XP の通常表示モード（カテゴリー表示モード）を前提に説明します。

1 ［スタート］メニューから［コントロールパネル］を選択し、［ネットワークとインターネット接続］を選択します。

2 ［ネットワーク接続］をクリックします。

3 ［ローカルエリア接続］アイコンを右クリックし、［プロパティ］を選択します。

4 ［インターネットプロトコル（TCP/IP）］を選択し、［プロパティ］ボタンをクリックします。

5 ［次の IP アドレスを使う］、［次の DNS サーバアドレスを使う］にチェックをつけます。

6 IP アドレス、サブネットマスク、デフォルトゲートウェイ、DNS サーバのアドレスを入力します。

[次の IP アドレスを使う]
チェックを付けます。

[IP アドレス]
このパソコンに割り当てる IP アドレスを入力します。
IP アドレスは、本商品や LAN 内の他のパソコン、およびネットワーク機器と重複しないように設定してください。

[サブネットマスク]
本商品 LAN 側ポートに設定されているものと同じサブネットマスクを入力します。

[デフォルトゲートウェイ]
デフォルトゲートウェイアドレスを入力します。本商品をデフォルトゲートウェイにする場合は、本商品の LAN 側ポートに設定されている IP アドレスを入力します。

[次の DNS サーバーのアドレスを使う]
チェックを付けます。

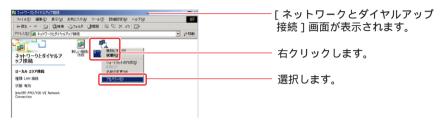
[優先 DNS サーバー]
DNS サーバアドレスを入力します。本商品を DNS サーバにすると場合は、本商品の LAN 側ポートに設定されている IP アドレスを入力します。
購入時は、本商品の LAN 側ポートの IP アドレスは「192.168.1.1」が設定されています。

6 ［OK］ボタンをクリックします。

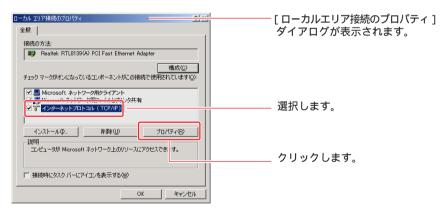
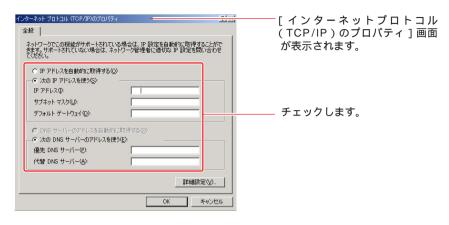
7 以上で設定は終了です。

Windows® 2000

1 **［スタート］メニューから［設定］－［コントロールパネル］を選択し、［ネットワークとダイヤルアップ接続］アイコンをダブルクリックします。**

2 **［ローカルエリア接続］アイコンを右クリックし、［プロパティ］選択します。**

※お使いのパソコンに複数のLANボード/カードが設置されているときは、本商品との接続に使用しているLANボード/カードの［ローカルエリア接続］を選択してください。

3 **［インターネットプロトコル（TCP/IP）］を選択し、［プロパティ］ボタンをクリックします。**

8
資料

4 [次の IP アドレスを使う]、[次の DNS サーバのアドレスを使う] にチェックをつけます。

5 IP アドレス、サブネットマスク、デフォルトゲートウェイ、DNS サーバのアドレスを入力します。

IP アドレスを自動的に取得する(O)
次の IP アドレスを使う(S):
IP アドレス(I): 192 168 1 3
サブネット マスク(U): 255 255 255 0
デフォルト ゲートウェイ(D): 192 168 1 1
DNS サーバーのアドレスを自動的に取得する(B)
次の DNS サーバーのアドレスを使う(E):
優先 DNS サーバー(P): 192 168 1 1
代替 DNS サーバー(A):

[次の IP アドレスを使う]
チェックを付けます。

[IP アドレス]
このパソコンに割り当てる IP アドレスを入力します。
IP アドレスは、本商品や LAN 内の他のパソコン、およびネットワーク機器と重複しないように設定してください。

[サブネットマスク]
本商品 LAN 側ポートに設定されているものと同じサブネットマスクを入力します。

[デフォルトゲートウェイ]
デフォルトゲートウェイアドレスを入力します。本商品をデフォルトゲートウェイにする場合は、本商品の LAN 側ポートに設定されている IP アドレスを入力します。

[次の DNS サーバーのアドレスを使う]
チェックを付けます。

[優先 DNS サーバー]

DNS サーバアドレスを入力します。本商品を DNS サーバにすると場合は、本商品の LAN 側ポートに設定されている IP アドレスを入力します。
購入時は、本商品の LAN 側ポートの IP アドレスは「192.168.1.1」が設定されています。

6 ［OK］ボタンをクリックします。

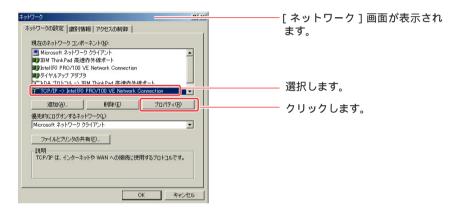
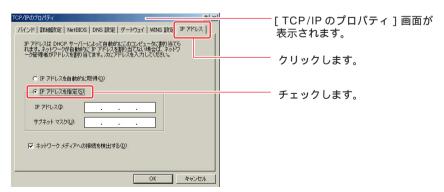
7 以上で設定は終了です。

Windows® Me/98

ここでは、Windows® Me を例にして、IP アドレスの設定を行います。Windoes® 98 をお使いのお客様は同様の手順で設定してください。

1　［スタート］メニューから［設定］－［コントロールパネル］を選択し、［ネットワーク］アイコンをダブルクリックします。

※コントロールパネルに［ネットワーク］が表示されていないときは、コントロールパネルのウィンドウの左側にある［すべてのコントロールパネルのオプションを表示する］をクリックしてください。

2　［TCP/IP］を選択し、［プロパティ］ボタンをクリックします。

3　［IP アドレス］タブをクリックし、［IP アドレスを指定］にチェックを付けます。

4 [IP アドレス]、[サブネットマスク] を入力します。

[IP アドレスを指定]

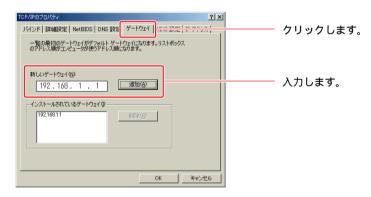
チェックを付けます。

[IP アドレス]

このパソコンに割り当てるIP アドレスを入力します。
IP アドレスは、本商品やLAN 内の他のパソコン、およびネットワーク機器と重複しないように設定してください。

[サブネットマスク]

本商品LAN 側ポートに設定されているものと同じサブネットマスクを入力します。

5 [ゲートウェイ] タブをクリックします。[新しいゲートウェイ] にアドレスを入力し、[追加] ボタンをクリックします。

[新しいゲートウェイ]

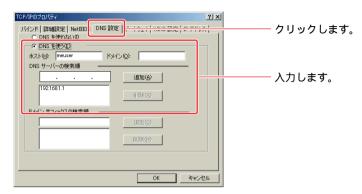
本商品のLAN 側ポートに設定されているIP アドレスを入力します。
購入時は、本商品のLAN 側ポートのIP アドレスは、「192.168.1.1」が設定されています。

[[追加] ボタン]

[新しいゲートウェイ] を入力した後で、クリックします。

[インストールされているゲートウェイ]

ゲートウェイとして設定されているIP アドレスが表示されます。

6 ［DNS 設定］タブをクリックします。
［DNS サーバーの検索順］にアドレスを入力し、［追加］ボタンをクリックします。

［DNS を使う］
チェックを付けます。

［ホスト］
パソコンのホスト名を入力します。

［DNS サーバーの検索順］
DNS サーバアドレスを入力します。本商品を DNS サーバにする場合は、本商品の LAN 側ポートに設定されている IP アドレスを入力します。
購入時は、本商品の LAN 側ポートの IP アドレスは「192.168.1.1」が設定されています。

［［追加］ボタン］
［DNS サーバーの検索順］の IP アドレスを入力した後で、クリックします。

7 ［OK］ボタンをクリックします。
Windows® の再起動を促すメッセージが表示されたら、［はい］ボタンをクリックします。

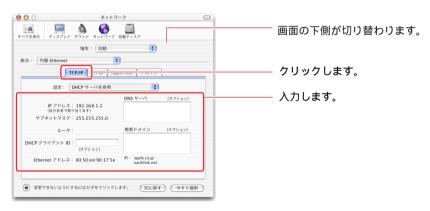
8 以上で設定は終了です。

Mac OS® X

1 **画面左上のアップルメニューから、［システム環境設定］を選択します。**

2 **ネットワークをクリックします。**

3 **［TCP/IP］タブをクリックし、IP アドレスやサブネットマスクなどを入力します。**

8
資料

[表示]
　「内蔵 Ethernet」を選択します。

[設定]
　「手入力」を選択します。

[IP アドレス]
　このパソコンに割り当てるIP アドレスを入力します。
　IP アドレスは、本商品やLAN 内の他のパソコン、およびネットワーク機器と重複しないように設定してください。

[サブネットマスク]
　本商品LAN 側ポートに設定されているものと同じサブネットマスクを入力します。

[ルータ]
　本商品のLAN 側ポートに設定されているIP アドレスを入力します。

[DNS サーバ]
　DNS サーバアドレスを入力します。本商品を DNS サーバにするときは、本商品のLAN 側ポートに設定されているIP アドレスを入力します。
　購入時は、本商品のLAN 側ポートのIP アドレスは「192.168.1.1」が設定されています。

[検索ドメイン]
　プロバイダからドメイン名を指定されているときは、ドメイン名を入力します。

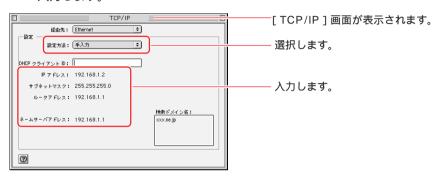
4 ［今すぐ適用］ボタンをクリックします。

5 以上で設定は終了です。

Mac OS® (8～9)

ここでは、MacOS®9を例にしてIPアドレスの設定を行います。他のバージョンをお使いのお客さまも、同様の手順で設定してください。

1 画面左上のアップルメニューから、［コントロールパネル］－［TCP/IP］を選択します。

2 設定方法から［手入力］を選択し、IPアドレスやサブネットマスクなどを入力します。

[経由先]
「Ethernet」を選択します。

[設定方法]
「手入力」を選択します。

[IPアドレス]
このパソコンに割り当てるIPアドレスを入力します。
IPアドレスは、本商品やLAN内の他のパソコン、およびネットワーク機器と重複しないように設定してください。

サブネットマスク
本商品LAN側ポートに設定されているものと同じサブネットマスクを入力します。

[ルータアドレス]
本商品のLAN側ポートに設定されているIPアドレスを入力します。

[ネームサーバアドレス]
本商品のLAN側ポートに設定されているIPアドレスを入力します。
購入時は、本商品のLAN側ポートのIPアドレスは「192.168.1.1」が設定されています。

[検索ドメイン名]
プロバイダからドメイン名を指定されている場合は、ドメイン名を入力します。

3 ダイアログの左上のクローズボックスをクリックします。
設定内容の保存を確認するメッセージが表示されたら、［保存］ボタンをクリックします。

4 以上で設定は終了です。

IP アドレスの再取得

パソコンのIP アドレスをDHCP サーバから取得する設定の場合、以前に割り当てられたIP アドレスを無効にして、IP アドレスを取得し直す方法を解説します。

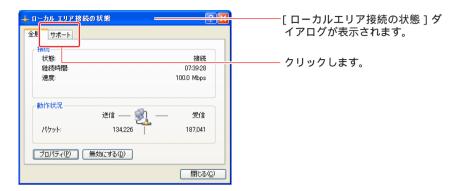
Windows® XP

ここでは、WIndows® XP の通常表示モード（カテゴリー表示モード）を前提に説明します。

1 ［スタート］－［コントロールパネル］－［ネットワークとインターネット接続］を選択します。

2 ［ネットワーク接続］をクリックします。

3 ［ローカルエリア接続］を右クリックし、［状態］を選択します。

4 ［サポート］タブをクリックします。

5 ［修復］ボタンをクリックします。それまで設定されていたIP アドレスが無効になり、DHCP サーバから新しいIP アドレスが割り当てられます。

Windows® 2000

1 **［スタート］メニューから［プログラム］－［アクセサリ］－［コマンドプロンプト］を選択します。**

2 **［ipconfig /renew］と入力して［Enter］キーを押しますそれまで設定されていたIPアドレスが無効になり、DHCPサーバから新しいIPアドレスが割り当てられます。**

Windows® Me/98

ここでは、Windows® Meを例にします。

1 **［スタート］メニューから［ファイル名を指定して実行］を選択します。**

2 **［名前］欄に「winipcfg」と入力して［OK］ボタンをクリックします。**

3 **［解放］ボタンをクリックし、続けて［書き換え］ボタンをクリックします。**
それまで設定されていたIPアドレスが無効になり、DHCPサーバから新しいIPアドレスが割り当てられます。

Mac OS®/Mac OS® X

1 **Macintosh® を再起動します。**
再起動時に、DHCP サーバから新しいIP アドレスが割り当てられます。

MAC アドレスの確認

本商品のDHCPサーバ機能では、同じパソコンに装着されている複数のLANボード/カードに同じIPアドレスを割り当てることができます。このような場合にMACアドレスを確認する方法を解説します。

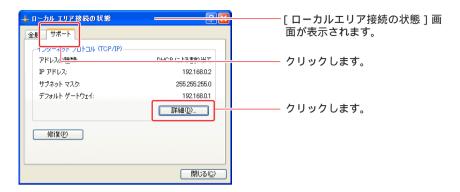
Windows® XP

ここでは、Windows® XPの通常表示モード（カテゴリー表示モード）を前提に説明します。

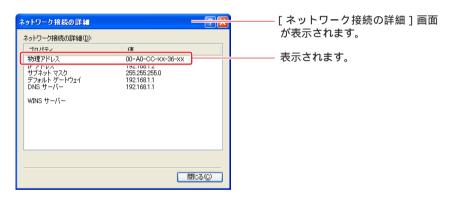
1 **［スタート］－［コントロールパネル］－［ネットワークとインターネット接続］を選択します。**

2 **［ネットワーク接続］をクリックします。**

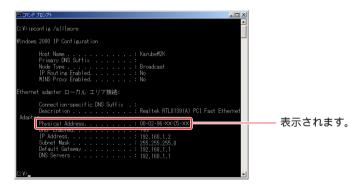
3 **［ローカルエリア接続］を右クリックし、［状態］を選択します。**

4 ［サポート］タグをクリックし、［詳細］ボタンをクリックします。

5 ［物理アドレス］欄に、現在使用している LAN アダプタの MAC アドレスが表示されます。

6 以上で確認作業は終了です。

Windows® 2000

1 **［スタート］メニューから［プログラム］－［アクセサリ］－［コマンドプロンプト］を選択します。**

2 **［ipconfig /all］と入力して、［Enter］キーを押します。**

3 **［Physical Address］欄に現在使用している、LAN アダプタの MAC アドレスが表示されます。**

Windows® Me/98

ここでは、Windows® Me を例にして、MACアドレスを確認する方法について説明します。Windows® 98をお使いのお客さまも同様の手順でご確認ください。

1 **［スタート］メニューから［ファイル名を指定して実行］を選択します。**

2 **［名前］欄に［winipcfg］と入力し、［OK］ボタンをクリックします。**

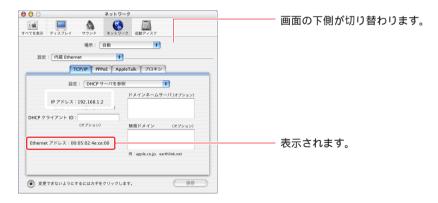
3 **使用するLANアダプタを選択します。［アダプタアドレス］欄に選択したLANアダプタのMACアドレスが表示されます。**

Mac OS® X

1　**画面左上のアップルメニューから、［システム環境設定］を選択します。**

2　**［ネットワーク］をクリックします。**

3　**［Ethernet アドレス］欄に現在使用している LAN アダプタの MAC アドレスが表示されます。**

8
資料

Mac OS® (8～9)

ここでは、MacOS® 9を例にして、MACアドレスを確認する方法について説明します。MacOS® 8をお使いのお客さまはも同様の手順でご確認ください。

1 **画面左上のアップルメニューから、［Apple システム・プロフィール］を選択し、［ネットワーク概略］→［AppleTalk］の順に▷をクリックします。**

2 **［ハードウェアアドレス］欄に、現在使用しているLANアダプタのMACアドレスが表示されます。**

用語解説

■ ADSL（Asymmetric Digital Subscriber Line：非対称ディジタル加入者回線）
通信速度が上り方向と下り方向で非対称なデータ通信技術です。家庭に普及しているアナログの電話線を使い、インターネットへの高速で安価な接続環境を提供します。

■ ALG（Application Layer Gateway：アプリケーション層ゲートウェイ）
オンラインゲームやチャットなどの特定アプリケーションやプロトコルで、経路上に存在するゲートウェイが内部ネットワークと外部ネットワークの橋渡しをする機能です。

■ bps（bits per second）
通信速度の単位です。1 秒間に転送できるビット数をあらわします。

■ B フレッツ
NTT 東日本・ NTT 西日本が提供する、光ファイバをアクセスラインとするインターネット通信料完全定額制サービスです。光ファイバならではの高速通信が利用できます。

■ DHCP（Dynamic Host Configuration Protocol）
コンピュータやネットワーク機器のアドレスやサブネットマスクなどの IP 設定を、自動構成するプロトコルです。

■ DMZ（DeMilitarized Zone：非武装地帯）
インターネットとの通信を制限しないネットワークセグメントのこと。ファイアウォールやルータによって配置、主にインターネットに公開するサーバを設置します。

■ DNS（Domain Name System）
IP アドレスやドメイン名を管理する機能です。ホスト名から IP アドレス、または IP アドレスからホスト名を調べることができます。

■ DoS 攻撃（Denial of Service Attack）
ネットワークのサービス妨害攻撃のことです。
ネットワークに接続されるコンピュータに大量のパケットを送信するなどして、対象のコンピュータの負荷を高くし、正常なサービスを提供できなくしたり利用不可の状態にしたりします。

■ Dynamic DNS（ダイナミック DNS）
DNS が使うホスト名と IP アドレスとの対応を動的に変更する技術のことです。
ホストの IP アドレスが変わっても、ホスト名と IP アドレスの対応表を更新することで、ホスト名を維持することができます。

■ **IGMP（Internet Group Management Protocol）**
マルチキャストを行うルータが、マルチキャストグループの情報を得るために使う、ルータと端末間のプロトコルです。ルータが管理するネットワーク内にある端末が、マルチキャストを受けるグループに参加・脱退したり、ルータ間でグループの情報をやり取りするときに使われます。

■ **IKE（Internet Key Exchange）**
IPSec による通信では、接続元と接続先が相互に通信を開始する前に、暗号の種類や暗号鍵を取り決めます。この取り決めの交換と、交換する相手の認証に使用される自動鍵管理プロトコルのことです。

■ **IPSec（IP Security）**
暗号通信のための規格のひとつです。IPSec では、IP のパケットを暗号化して送受信します。

■ **IP アドレス**
TCP/IP を使ったネットワーク上で、コンピュータなどを識別するためのアドレスです。IP アドレスは 32bit の値を持ち、8bit ずつ 10 進法で表現した数値を、ピリオドで区切って表現します。

■ **IP マスカレード**
→ NAPT（Network Address Port Translation）

■ **LAN（Local Area Network）**
ひとつの建物内などに接続された、複数のパソコンやプリンタなどで構成されている比較的小規模なネットワークです。

■ **MAC アドレス**
ネットワークアダプタなどのハードウェアに付けられた固有のアドレスです。ハードウェアの利用者が、このアドレスを決めることはできません。

■ **NAT（Network Address Translation）**
プライベート IP アドレスを、1 対 1 でグローバル IP アドレスに変換する機能です。
インターネットに接続するパソコンに直接グローバル IP アドレスを割り当てて使用すると、外部からの攻撃にさらされやすくなる危険性があります。このため、パソコンにはプライベート IP アドレスを割り当てておき、インターネットに接続するときだけルータを介してグローバル IP アドレスを割り当てます。

■ **NAPT（Network Address Port Translation）**
1 つのグローバル IP アドレスに複数のプライベート IP アドレスを動的に割り当てる機能です。「IP マスカレード」とも呼ばれます。

■ **NTP（Network Time Protocol）**
ネットワークを介して、コンピュータの内部時計を正しく調整するためのプロトコルです。ネットワーク上で時刻情報を提供する NTP サーバに、ネットワーク上の他のコンピュータが内部時計を同期させることによって調整が行われます。

■ **Numbered**
ルータのLAN側ポートとWAN側ポートに、それぞれ異なるIPアドレスを割り当てて運用する接続方式です。

■ **Ping**
コンピュータ間の接続が正常に行えるかを試験するプログラムです。

■ **PPPoE（Point to Point Protocol over Ethernet）**
フレッツ・ADSLなどの常時接続型サービスで使用されるユーザ認証技術の1つです。PPPoEでは、Ethernet上でPPPによる接続を行います。

■ **PPTP（Point to Point Tunneling Protocol）**
Microsoft社によって提案された、暗号通信のためのプロトコルのひとつです。

■ **RIP（Routing Information Protocol）**
TCP/IPネットワークにおいて、動的なルーティング制御を行うためのプロトコルです。ルータが到達不能経路を自動的に検出するなど、経路情報を動的に更新することができます。

■ **SNMP（Simple Network Management Protocol）**
コンピュータ、ルータなどをTCP/IPネットワーク上で監視したり制御したりするためのプロトコルです。このプロトコルによって管理されるネットワーク機器は、状態を表す管理情報データベース（MIB）を持ちます。管理する側の機器は、MIBに基づき設定します。

■ **SSID（Service Set ID）**
無線LANに関する国際規格であるIEEE802.11で、固定した相手先との接続を実現するための識別データです。32バイト長のデータで、アクセスポイントと端末間での接続処理の中で送受信される制御データの1つとなります。アクセスポイントと端末でSSIDが一致しないと、接続が確立しない仕組みになっています。

■ **TCP/IP（Transmission Control Protocol/Internet Protocol）**
インターネットやLANで一般的に使われるプロトコルです。

■ **Unnumbered**
複数グローバルIPアドレスのサービスのことです。
プロバイダから割り当てられた複数のグローバルIPアドレスをコンピュータに割り当て、使うことができます。

■ **UPnP（Universal Plug and Play）**
インターネットで標準になっている技術を基にして、家庭内にあるパソコンやAV機器、電話、家電製品などをネットワークにつなぐだけで利用可能にすることを目指した技術です。

■ **VPN（Virtual Private Network）**
インターネットなどのネットワーク上で論理的なグループを構成し、そのグループ間で閉域性を保つ仕組みを設けたネットワークのことです。ネットワーク網には不特定多数のユーザが接続していますが、VPNを構築することで、特定のユーザ間だけで通信が可能になります。

■ **WAN（Wide Area Network）**
離れた場所のLAN同士を、電話回線や専用線を介して接続するネットワークのことです。

■ **WEP（Wired Equivalent Privacy）**

無線LANの国際規格IEEE802.11で採用されている暗号化技術です。アクセスポイントとコンピュータの両方で、同じ文字列からなる「キー（鍵）」を設定して、そのキーを使いデータの暗号化や複号化が行われます。

■ **Webブラウザ**

ホームページなどを見るためのアプリケーションソフトのことです。Internet ExplorerやNetscape Navigator® がよく使われています。

■ **10BASE-T**

Ethernetの通信方式の１つです。10Mbit/sの伝送速度を持ちます。

■ **100BASE-TX**

Ethernetの通信方式の１つです。100Mbit/sの伝送速度を持ちます。

■ **アクセスポイント**

無線LANと有線LANの間の通信の中継や、無線LAN同士の中継をするネットワーク機器です。
無線LANアダプタを取り付けたコンピュータはアクセスポイントとの間で無線通信をします。

■ **クライアント**

LANを構成するコンピュータの中で、主にサーバからの資源やサービス（ファイル/データベース/メール/プリンタなど）を受けるコンピュータのことです。

■ **グローバルIPアドレス**

インターネット上の通信相手を特定するために使うIPアドレスの種類のひとつです。
グローバルIPアドレスは、インターネット上で唯一のアドレスで、同じアドレスは存在しません。

■ **サーバ**

LANを構成するコンピュータの中で、主にクライアントに資源やサービス（ファイル/データベース/メール/プリンタなど）を提供するコンピュータのことです。例えば、インターネット上ではWebサーバがホームページを提供します。

■ **ステートフル・パケット・インスペクション（SPI）**

ファイアウォールを通過するパケットのデータを読み取って内容を判断し、動的にポートを開放したり閉鎖したりする機能です。

■ **ファイアウォール**

外部から内部のコンピュータネットワークへ侵入されることを防ぐシステムです。内部のネットワークと外部のネットワークの境界でデータを監視し、不正なアクセスを検出したり遮断したりします。このシステムが組み込まれた機器を「ファイアウォール」と呼ぶこともあります。

■ **ファームウェア**

ハードウェアを動作させるプログラムです。

■ **プライベートIPアドレス**

インターネットと直接接続されていないネットワークで使うIPアドレスです。

■ **フレッツ・ADSL**

NTT地域会社（東日本、西日本）から提供されている、加入電話回線または専用回線を使ったADSL接続サービスです。フレッツ・ADSLではユーザ認証にPPPoEが使われています。

■ **プロトコル**

ネットワーク上の機器間で正しく通信をするための決まりごとのことです。

■ **ホスト**

インターネットでは、Webサーバやメールサーバなどの各種サービスを行うコンピュータをホストとして扱います。

■ **ポート**

IPアドレスの下に設けられた補助的なアドレスのことです。TCP/IPで通信を行うコンピュータは、複数のコンピュータと同時に通信するために、複数のポートを利用します。

■ **マルチキャスト**

ネットワーク内で、指定した複数の相手に同じデータを送信することです。TCP/IPネットワークでは、複数のあて先に対して1つのIPアドレス（マルチキャストアドレス）を指定して、1回だけデータを送信すれば、通信経路上のルータがあて先に応じてデータを複製して送信します。

■ **ルータ**

複数のネットワークを相互に接続し、データの転送先や経路を選択する装置のことです。

■ **ローカルサーバ**

LAN側に設置した特定のサーバをインターネット上からアクセス可能にする機能です。TCP、UDPのポート番号ごとに転送先のLAN側のコンピュータを指定します。オンラインゲームやチャットなどを行うときにも使います。

設定記入シート

保守のための資料として、設定内容を記入し、大切に保管してください。プロバイダの認証パスワードやメールのパスワードは、お客様の個人情報となります。記入された際は、本設定記入シートのお取り扱いにご注意ください。

設定ページログイン	ログインユーザ名	
	ログインパスワード	

サイドバー	設定画面タイトル		設定項目	設定データ
かんたんウィザード設定	インターネット接続	PPPoE接続	接続ユーザ名	
			接続パスワード	
		PPPoE以外の接続	IPアドレス	自動取得／固定IPアドレス
			固定IPアドレス	
			IPアドレス	
			サブネットマスク	
			デフォルトゲートウェイ	
			プライマリDNSサーバ	
			セカンダリDNSサーバ	
	VPN接続	PPTPクライアント	接続先のホスト名またはIPアドレス	
			接続ユーザ名	
			接続パスワード	
		PPTPサーバ	ユーザの追加	「ユーザリスト」P.8-52
			リモートアドレス範囲	開始:
				終了:
		IPSec	接続先のホスト名またはIPアドレス	
			サブネットアドレス	
			サブネットマスク	
			共通鍵	

※次ページに続きます。

サイドバー	設定画面タイトル		設定項目	設定データ
ネットワーク詳細設定	WANポート	詳細設定	MACアドレス	
			MTU	
			IPアドレス	自動／固定
			IPアドレスを自動取得する場合	
			DNSサーバ	自動取得／固定設定
			DNSサーバを固定設定する場合	
			プライマリDNSサーバ	
			セカンダリDNSサーバ	
			IPアドレスを固定設定する場合	
			IPアドレス	
			サブネットマスク	
			デフォルトゲートウェイ	
			プライマリDNSサーバ	
			セカンダリDNSサーバ	
			LAN側グローバルネットワーク（Unnumbered接続）	
			ネットワークアドレス	
			サブネットマスク	
			NAPT	有効／無効
			デバイスメトリック	
	LAN	詳細設定	MACアドレス	
			IPアドレス	有効／無効
			DHCPサーバ	
			割り当て開始アドレス	
			割り当て終了アドレス	
			割り当てサブネットマスク	
			WINSサーバ	（分）
			リース期間（分）	
			クライアントにホスト名が設定されていないとき自動的にホスト名を割り当てる	
			デバイスメトリック	

8 資料

サイドバー	設定画面タイトル		設定項目	設定データ
ネットワーク詳細設定	PPPoE接続1	詳細設定	MTU	
			接続ユーザ名	
			接続パスワード	
			自動切断	有効／無効
			自動切断までの時間（分）	（分）
			PAP認証を許可する（PAP）	有効／無効
			CHAP認証を許可する（CHAP）	有効／無効
			IPアドレスを自動取得する	自動取得／固定設定
			サブネットマスクを置き換える	有効／無効
			サブネットマスク	
			IPアドレスを固定設定する	
			IPアドレス	
			サブネットマスク	
			デフォルトゲートウェイ	
			DNSサーバアドレス	自動取得／固定設定
			DNSサーバを固定設定する	
			プライマリDNSサーバ	
			セカンダリDNSサーバ	
			デバイスメトリック	
			NAPT	有効／無効
			LAN側グローバルネットワーク（Unnumbered接続）	
			ネットワークアドレス	
			サブネットマスク	
	PPPoE接続2	詳細設定	MTU	
			接続ユーザ名	
			接続パスワード	有効／無効
			PPPoE2～4は自動切断	
			PAP認証を許可する（PAP）	有効／無効
			CHAP認証を許可する（CHAP）	有効／無効
			IPアドレス	自動取得／固定設定
			IPアドレスを自動取得する	
			サブネットマスクを置き換える	有効／無効
			サブネットマスク	
			IPアドレスを固定設定する	
			IPアドレス	
			サブネットマスク	
			デフォルトゲートウェイ	
			DNSサーバアドレス	自動取得/固定設定

ネットワーク詳細設定	PPPoE接続2	詳細設定	DNSサーバを固定設定する	
			プライマリDNSサーバ	
			セカンダリDNSサーバ	
			デバイスメトリック	
			NAPT	
			LAN側グローバルネットワーク（Unnumbered接続）	
			ネットワークアドレス	
			サブネットマスク	

8
資料

サイドバー	設定画面タイトル		設定項目	設定データ
ネットワーク詳細設定	VPN PPTPクライアント	詳細設定	MTU	
			接続先のホスト名またはIPアドレス	
			接続ユーザ名	
			接続パスワード	
			自動切断までの時間（分）	（分）
			PAP認証を許可する（PAP）	有効／無効
			CHAP認証を許可する（CHAP）	有効／無効
			MS-CHAP認証を許可する(MS-CHAP)	有効／無効
			MS-CHAP v2認証を許可する（MS-CHAP v2）	有効／無効
			暗号化を必ず要求する（サーバが拒否したときは切断）	有効／無効
			暗号化を許可する (MPPE-40Bit)	有効／無効
			最強の暗号化を許可する (MPPE-128Bit)	有効／無効
			MPPE暗号化モード	MPPE-Stateless / MPPE-Stateful
			IPアドレス	自動取得／固定設定
			IPアドレスを固定設定する	
			IPアドレス	
			サブネットマスクを置き換える	有効／無効
			DNSサーバアドレス	自動取得／固定設定
			DNSサーバアドレスを固定設定する	
			プライマリDNSサーバ	
			セカンダリDNSサーバ	
			デバイスメトリック	
			NAPT有効／無効	有効／無効
	VPN PPTPサーバ	詳細設定	PPTPサーバ	（分）
			自動切断までの時間	有効／無効
			認証が必要	有効／無効
			暗号化が必要	有効／無効
			PAP	有効／無効
			CHAP	有効／無効
			MS-CHAP-V1	有効／無効
			MS-CHAP-V2	有効／無効
			MPPE-40	有効／無効
			MPPE128	Stateful／Stateless
			MPPE暗号化モード	
			リモートアドレス範囲	
			開始	
			終了	

サイドバー	設定画面タイトル			設定項目	設定データ
ネットワーク詳細設定	VPN IPSec		詳細設定	接続先のホスト名またはIPアドレス	
				ローカルサブネット	
				サブネットアドレス	
				サブネットマスク	
				リモートサブネット	
				サブネットアドレス	
				サブネットマスク	
				データ圧縮(IPCOMPプロトコル)	有効/無効
				鍵交換方式	自動(IKE)/手動
				鍵交換自動設定	
				IPSec IKE, Phase 1	
				モード	メインモード/アグレッシブモード
				メインモード設定	
				接続試行回数	無制限/1/2/3/4/8/16/24/32/48/64
				ライフタイム(秒:1-28800)	
				Rekey Margin (秒:1-540)	
				Rekey Fuzz (パーセンテージ:1-200)	
				認証アルゴリズム	共通鍵方式/公開鍵方式
				共通鍵方式	
				公開鍵方式	
				暗号化アルゴリズム	DES-CBC/3DES-CBC
				ハッシュアルゴリズム	MD5/SHA1
				Diffie-Hellman Group	DH Group 1/DH Group 2/DH Group 5
				IPSec IKE, Phase 2	
				ライフタイム(秒:1-28800)	
				PFS有効	有効/無効
				Diffie-Hellman Group	Phase 1と同じ、DH Group 1、DH Group 2、DH Group 5
				暗号化アルゴリズム	なし/DES-CBC/3DES-CBC
				認証アルゴリズム	MD5/SHA1
				ハッシュアルゴリズム	MD5/SHA1
				デバイスメトリック	
				アグレッシブモード設定	
				接続試行回数	
				ライフタイム(秒:1-28800)	
				Rekey Margin (秒:1-540)	

サイドバー	設定画面タイトル		設定項目	設定データ
ネットワーク詳細設定	VPN IPSec	詳細設定	Rekey Fuzz (パーセンテージ:1-200)	
			認証アルゴリズム　共通鍵	
			暗号化アルゴリズム	DES-CBC/3DES-CBC/AES128-CBC/AES192-CBC/AES256-CBC
			ハッシュアルゴリズム	MD5/SHA 1
			デバイスメトリック	
			鍵交換手動設定	
			セキュリティインデックス	
			ローカル	
			リモート	
			ローカルとリモートで異なる暗号化キーを使用する	有効/無効
			IPSecプロトコル	ESP/AH
			暗号化アルゴリズム	なし/DES-CBC/3DES-CBC
			キー	
			認証アルゴリズム	SHA 1/MD 5
			キー	

サイドバー	設定画面タイトル	設定項目	設定データ
セキュリティ設定	セキュリティ	セキュリティレベル	最大／標準／最小
		IPフラグメントパケットを遮断する	有効／無効
	ローカルサーバ	新規作成	「ローカルサーバ」P.8-49
	DMZホスト	DMZホスト	有効／無効
		IPアドレス	
	リモートアクセス設定	Webサーバ	
		WEBサーバを外部に公開する（TCPポート80）	有効／無効
		WEBサーバを外部に公開する（TCPポート8080）	有効／無効
		設定画面を外部に公開する	有効／無効
		診断ツール	
		Ping(ICMP Echo Request)を許可する (PingおよびICMP Traceroute)	有効／無効
		Traceroute(UDP)を許可する	有効／無効
		オプション設定	
		USBカメラ画像を外部に公開する（8090）	有効／無効
		FTPサーバを外部に公開する（21）	有効／無効
		PHP対応WEBサーバを外部に公開する（TCPポート8008）	有効/無効
	セキュリティログ	ログイベント	
		許可した接続	有効/無効
		拒否した接続	有効/無効
		設定	
		ログ容量が一杯になったらログを停止する	有効/無効
	パケットフィルタ	新規作成	「パケットフィルタ」P.8-48

サイドバー	設定画面タイトル	設定項目	設定データ
URLフィルタ	URLフィルタ	フィルタ1	
		フィルタ2	
		フィルタ3	
		フィルタ4	
		フィルタ5	
		フィルタ6	
		フィルタ7	
		フィルタ8	
		フィルタ9	
		フィルタ10	

サイドバー	設定画面タイトル	設定項目	設定データ
カスタム設定	DNSサーバ	DNSエントリ1	ホスト名: IPアドレス:
		DNSエントリ2	ホスト名: IPアドレス:
		DNSエントリ3	ホスト名: IPアドレス:
		DNSエントリ4	ホスト名: IPアドレス:
		DNSエントリ5	ホスト名: IPアドレス:
		DNSエントリ6	ホスト名: IPアドレス:
		DNSエントリ7	ホスト名: IPアドレス:
		DNSエントリ8	ホスト名: IPアドレス:
		DNSエントリ9	ホスト名: IPアドレス:
		DNSエントリ10	ホスト名: IPアドレス:

サイドバー	設定画面タイトル	設定項目	設定データ
カスタム設定	DHCPサーバ	DHCP設定 LANポート	
		DHCPサーバ	有効／無効
		割り当て開始アドレス	
		割り当て終了アドレス	
		割り当てサブネットマスク	
		リース期間(分)	(分)
		WINSサーバ	
		クライアントリスト	「DHCPクライアントリスト」P.8-50
		クライアントにホスト名が設定されていないときにホスト名を自動的に割り当てる	有効／無効
	ルーティング	ルートの追加	「ルーティングテーブル」P.8-51
		RIP v1/v2	有効／無効
	ユーザ	フルネーム	
		ユーザ名	
		パスワード	
		管理者権限	有効／無効
		PPTPリモートアクセス	有効／無効
		ファイルサーバからのファイルの読み込み	
		ファイルサーバからのファイルの書き込み	
		USBカメラ	
		E-Mailアドレス	
		システム通知レベル	なし/エラー/警告/情報
		セキュリティ通知レベル	なし/エラー/警告/情報
		ユーザ追加	「ユーザリスト」P.8-52
	日付と時刻	日付	
		時刻	
		時刻の自動設定	有効／無効
		更新間隔	
		サーバアドレス	
	IPSec	IPSec	有効／無効
	UPnP	UPnP	
	システム設定	UPnPを適用する接続	
		WebCaster 800 ホスト名	有効／無効
		ローカルドメイン	
		NET BIOSワークグループ名	
		システム情報ページの表示の自動更新を行なう	有効／無効

サイドバー	設定画面タイトル	設定項目	設定データ
カスタム設定	システム設定	ネットワーク設定の変更時に確認を行なう	有効／無効
		システム通知レベル	なし/エラー/警告/情報
		システム通知レベル Syslogサーバアドレス	
		セキュリティ通知レベル	なし/エラー/警告/情報
		セキュリティ通知レベル Syslogサーバアドレス	
		SMTPメールサーバ	
		送信元メールアドレス	

サイドバー	設定画面タイトル	設定項目	設定データ
カスタム設定	ファイルサーバ	NetBIOSワークグループ名	
		詳細	
		タイプ	
		サイズ	
		共有	
	追加機能パッケージ	USBカメラ	有効/無効
		PHP対応Webサーバ	有効/無効
	ダイナミックDNS (DynDNS.org)	接続	
		オフライン	有効/無効
		ユーザ名	
		パスワード	
		ホスト名	
		ワイルドカード	有効/無効
		メールサーバ	
		バックアップメールサーバ	
	ダイナミックDNS (DP-21.NET)	有効にする	
		ユーザ名	
		パスワード	
		更新間隔	
	FTPサーバ	FTPサーバへのanonymousログインを許可する	有効/無効
	PHP対応Webサーバ	パーティション	
		ドキュメントルート	
	USBカメラ	オン/オフ	オン/オフ
		動画ビットレート	高/低

DHCPクライアントリスト

登録番号	ホスト名	IPアドレス	MACアドレス	リースタイプ
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				
26				
27				
28				
29				
30				
31				
32				

ルーティングテーブル

登録番号	デバイス	送信先	ゲートウェイ	ネットマスク	メトリック
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					
21					
22					
23					
24					
25					
26					
27					
28					
29					
30					
31					
32					

ユーザリスト

登録番号	フルネーム	ログインユーザー名	ログインパスワード	E-Mail	権限
1					管理者／PPTP
2					管理者／PPTP
3					管理者／PPTP
4					管理者／PPTP
5					管理者／PPTP
6					管理者／PPTP
7					管理者／PPTP
8					管理者／PPTP
9					管理者／PPTP
10					管理者／PPTP
11					管理者／PPTP
12					管理者／PPTP
13					管理者／PPTP
14					管理者／PPTP
15					管理者／PPTP
16					管理者／PPTP
17					管理者／PPTP
18					管理者／PPTP
19					管理者／PPTP
20					管理者／PPTP
21					管理者／PPTP
22					管理者／PPTP
23					管理者／PPTP
24					管理者／PPTP
25					管理者／PPTP
26					管理者／PPTP
27					管理者／PPTP
28					管理者／PPTP
29					管理者／PPTP
30					管理者／PPTP
31					管理者／PPTP
32					管理者／PPTP

当社ホームページでは、各種商品の最新の情報やバージョンアップサービスなどを提供しています。本商品を最適にご利用いただくために、定期的にご覧いただくことをお勧めします。

当社ホームページ：　http://www.ntt-east.co.jp/ced/
http://www.ntt-west.co.jp/kiki/

使い方等でご不明の点がございましたら、NTT通信機器お取扱相談センタへお気軽にご相談ください。

NTT 通信機器お取扱相談センタ

■NTT東日本エリアでご利用のお客様
（新潟県・長野県・山梨県・神奈川県以東の各都道県）
お問い合わせ先: フリーアクセス 0120−970413

■NTT西日本エリアでご利用のお客様
（富山県・岐阜県・愛知県・静岡県以西の各府県）
トークニイーナ
お問い合わせ先: 0120−109217

電話番号をお間違えにならないように、ご注意願います。

本2619-2（2005.4）
WBC 800トリセツ
PMN-05-4/WBC800-A